SÉCURITÉ DES RÉSEAUX
SYSTÈMES D'ANONYMATS

A. Guermouche

Plan

Introduction

MixNet

Onion Routing

DC-Net

Plan

Vie privée

Vie privée dans un environnement numérique

- Préoccupez-vous de votre vie privée en ligne ! Réponses communes :
  - Je n'ai rien à cacher.
  - Ceux qui s'inquiètent ont l'air suspects.
- Qu'en est-il de la vie privée dans d'autres aspects de la vie ? Utilisez-vous des rideaux ? Fermez-vous la porte ?
- L'anonymat est une étape vers la garantie de la vie privée.
  - Nous ne sommes pas anonymes sur Internet.
- Anonymat : La capacité à être non identifiable au sein d'un ensemble de sujets.

Types d'anonymat

Anonymat (*Anonimity*)

Incapacité à identifier une personne parmi un ensemble de sujets

- Différent de la notion de vie privée (le droit à être laissé seul)
- Pour rester anonyme, vous devez cacher vos activités parmi les activités similaires d'autres personnes
- On ne peut pas être anonyme en étant seul!

Non-reliabilité (*Unlinkability*)

Séparation entre l'action et l'identité de l'entité exécutant cette action

- Par exemple: l'expéditeur et son courrier électronique ne sont plus liés après l'écoute de la communication comme ils l'étaient avant.

Inobservabilité (*Inobservability*)

Incapacité de dire si une certaine action a eu lieu

Plan

Introduction

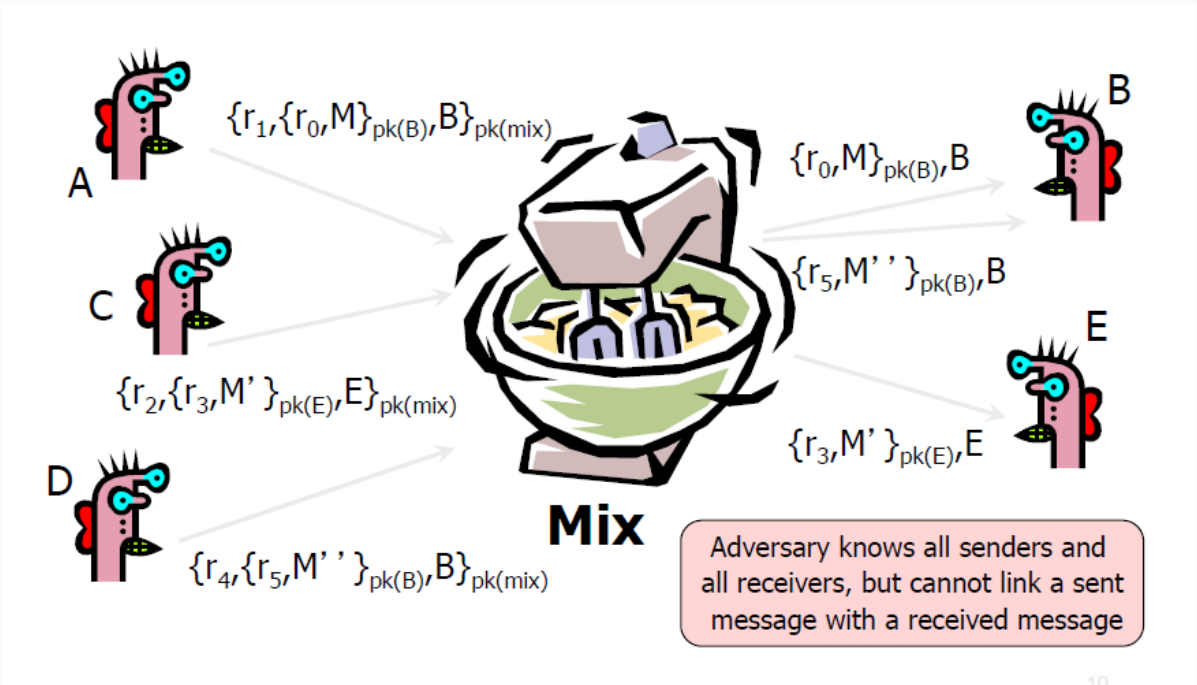
MixNet

Onion Routing

DC-Net

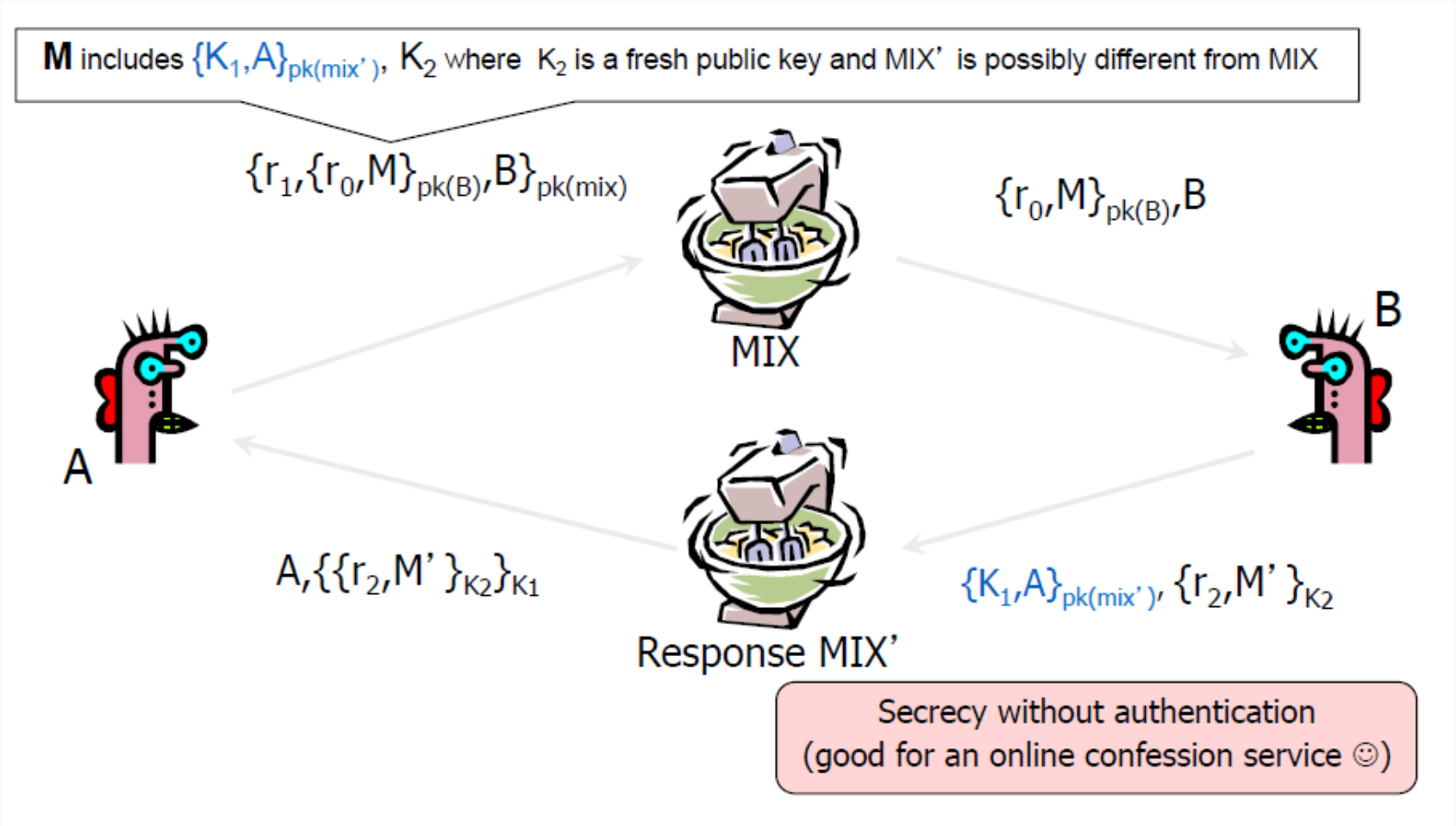
Mix de Chaum (1980)

- Première proposition de courrier électronique anonyme :
  - David Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms” , Communications de l’ACM, février 1981.
- Chiffrement à clé publique + réexpédition de confiance (Mix)
  - Un moyen de communication peu fiable
  - Les clés publiques utilisées comme pseudonymes persistants
- Les systèmes d’anonymat modernes utilisent les Mix comme élément de base



source http://sconce.ics.uci.edu/134-W18/slides/LEC15.pdf

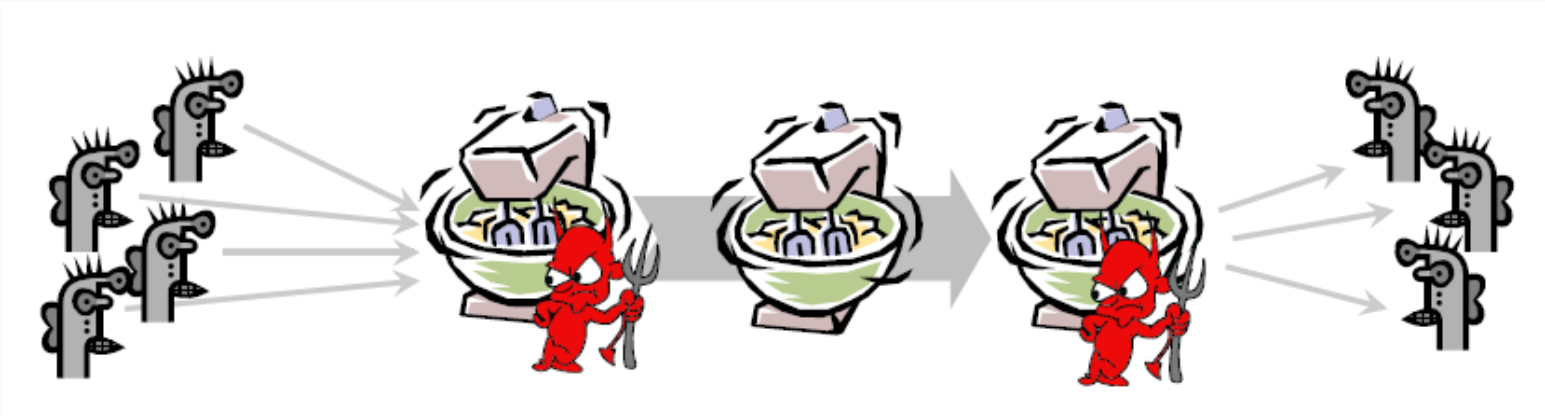
Adresse de retour anonyme



source http://sconce.ics.uci.edu/134-W18/slides/LEC15.pdf

Cascade de Mix

- Les messages sont envoyés via une séquence de Mix
  - Peut également former un réseau de Mix ("MixNet")
- Certains Mix peuvent être contrôlés par un attaquant, mais même un seul Mix sain garantit un certain anonymat
- Utiliser de la bufférisation (au niveau des Mix) pour déjouer les attaques par corrélation



source http://sconce.ics.uci.edu/134-W18/slides/LEC15.pdf

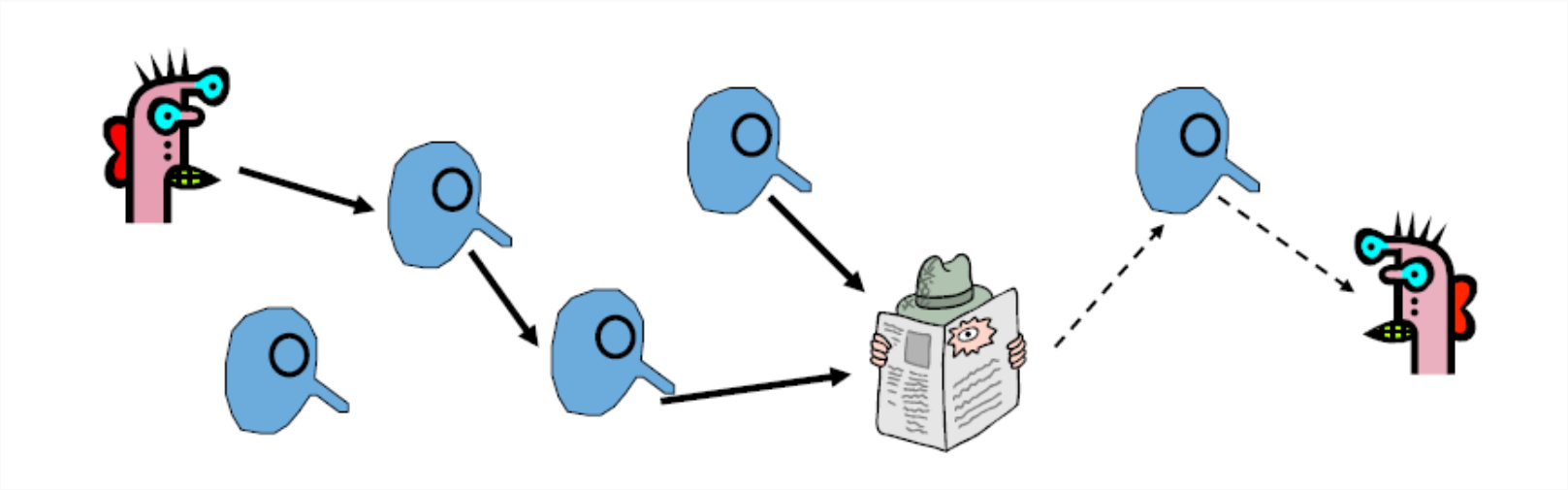
Discussion

Bilan

- Le chiffrement/déchiffrement asymétrique au niveau de chaque Mix est une opération coûteuse.
- Les mixnets de base ont une latence élevée
  - raisonnable pour le courrier électronique, mais pas pour la navigation anonyme sur le web
- Défi : réseau d'anonymat à faible latence
  - Utiliser la cryptographie à clé publique pour établir un "circuit" avec des clés symétriques par paires entre les intermédiaires
  - Utilisez ensuite le déchiffrement et le chiffrement symétrique pour déplacer les messages de données le long du circuits établi
  - Chaque noeud se comporte comme un Mix ; l'anonymat est préservé même si certains noeuds sont compromis

Plan

Routage randomisé

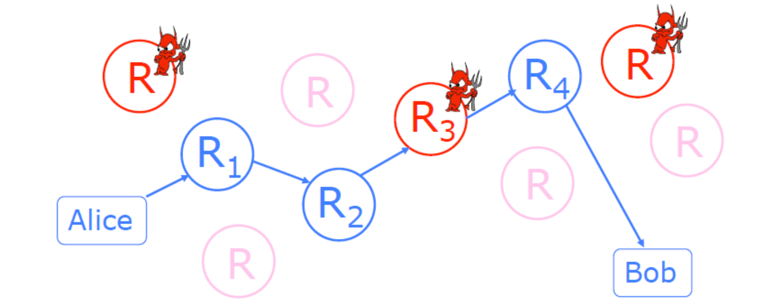


source http://sconce.ics.uci.edu/134-W18/slides/LEC15.pdf

Cacher les sources en acheminant les messages de manière aléatoire

- Technique populaire : Freenet, Onion routing
- Les routeurs ne savent pas si la source apparente d'un message est le véritable expéditeur ou un autre routeur

Onion Routing

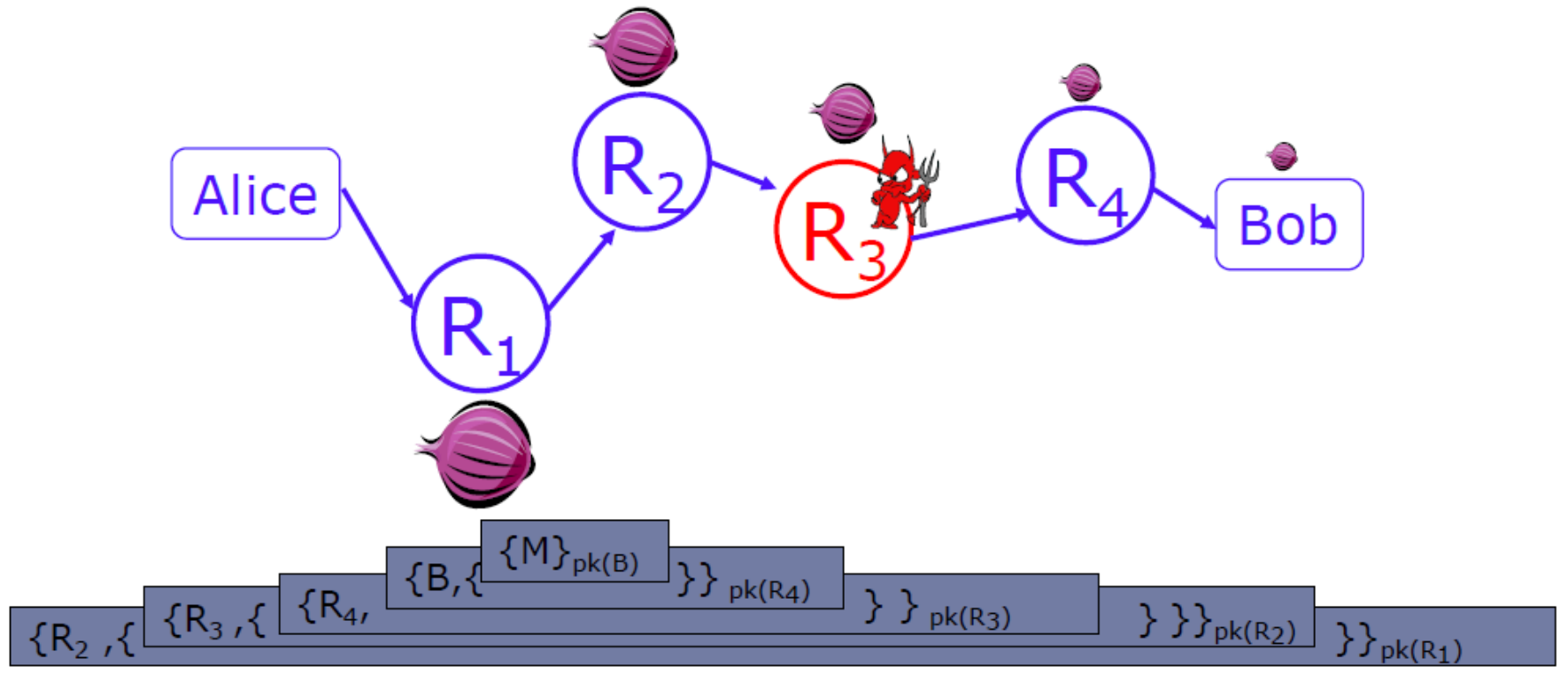


source http://sconce.ics.uci.edu/134-W18/slides/LEC15.pdf

L'expéditeur choisit une séquence aléatoire de routeurs

- Certains routeurs sont honnêtes, d'autres sont corrompus
- L'expéditeur contrôle la longueur du chemin

Détermination de la route



source http://sconce.ics.uci.edu/134-W18/slides/LEC15.pdf

- L'information de routage pour chaque est chiffrée avec la clé publique du routeur.
- Chaque routeur ne va connaître que son prédécesseur et son successeur.

Tor

Entités

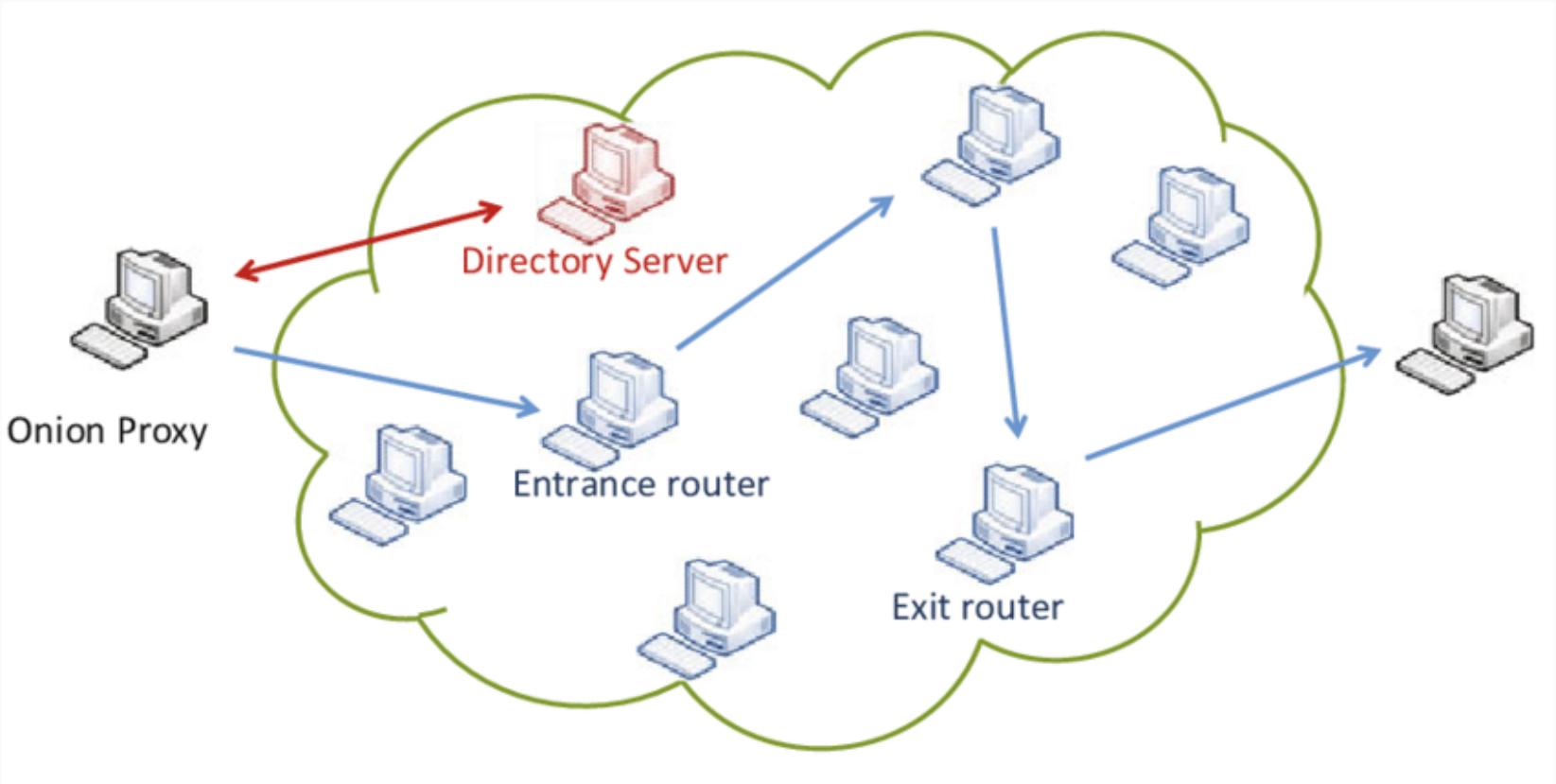
Onion Router (OR). Routeurs dans le réseau de superposition d'oignons.

Onion Proxy (OP). Proxy local de chaque utilisateur Tor.

Serveur d'annuaire. Entité de confiance fournissant un répertoire OR.

- Chaque OR maintient une connexion TLS avec tous les autres OR.
- Chaque OP maintient des connexions TLS avec ses OR d'entrée.
- Tor utilise des suites de chiffrement TLS avec des clés éphémères.
- TLS est utilisé pour l'authentification de l'OR et non pour le chiffrement de données de la charge utile !

Tor



source https://www.researchgate.net/figure/The-Onion-Router-Tor-communication_fig18_225230662

Clés de chiffrement

Clés

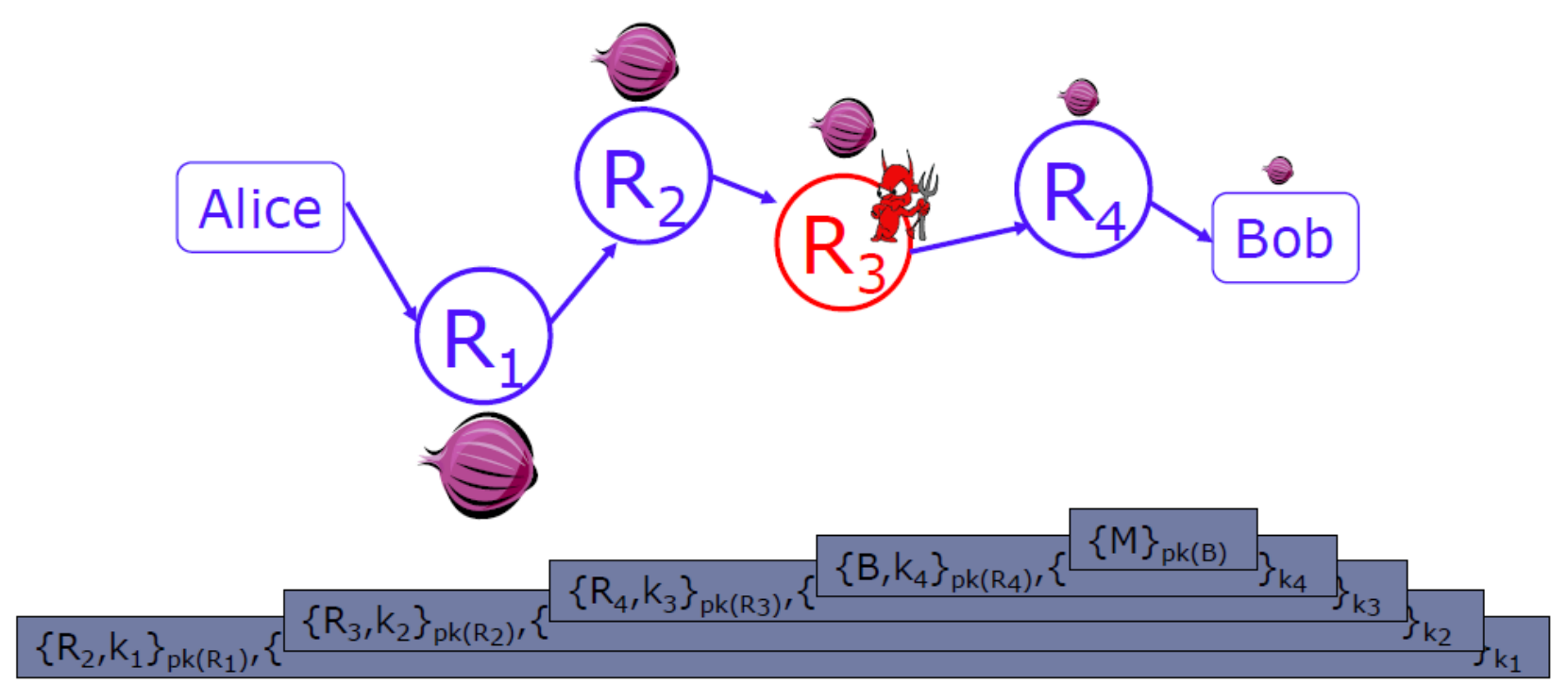
Clés asymétriques :

- Chaque OR publie une "clé d'identité de routeur" dans le répertoire.
- De plus, les serveurs d'annuaire ont :
  - une "Authority Identity Key" à long terme (stockée hors ligne) et
  - une "clé de signature de l'autorité" à moyen terme (3 à 12 mois).
  - Les OP n'ont pas de clés d'identité.

Clés symétriques :

- Toutes les connexions TLS utilisent des clés éphémères à court terme.
- Les clés de chiffrement des OR sont des clés éphémères à court terme ; Tor utilise AES128 en mode compteur pour le chiffrement entre OR.

Tor



source http://sconce.ics.uci.edu/134-W18/slides/LEC15.pdf

- Le client définit une clé de session avec chaque Onion router du circuit.
- Chaque routeur ne va connaître que son prédécesseur et son successeur ainsi qu'une clé de session partagée avec le client.

Plan

Dining Cryptographers

Une idée astucieuse pour rendre un message public d'une manière parfaitement intraçable.

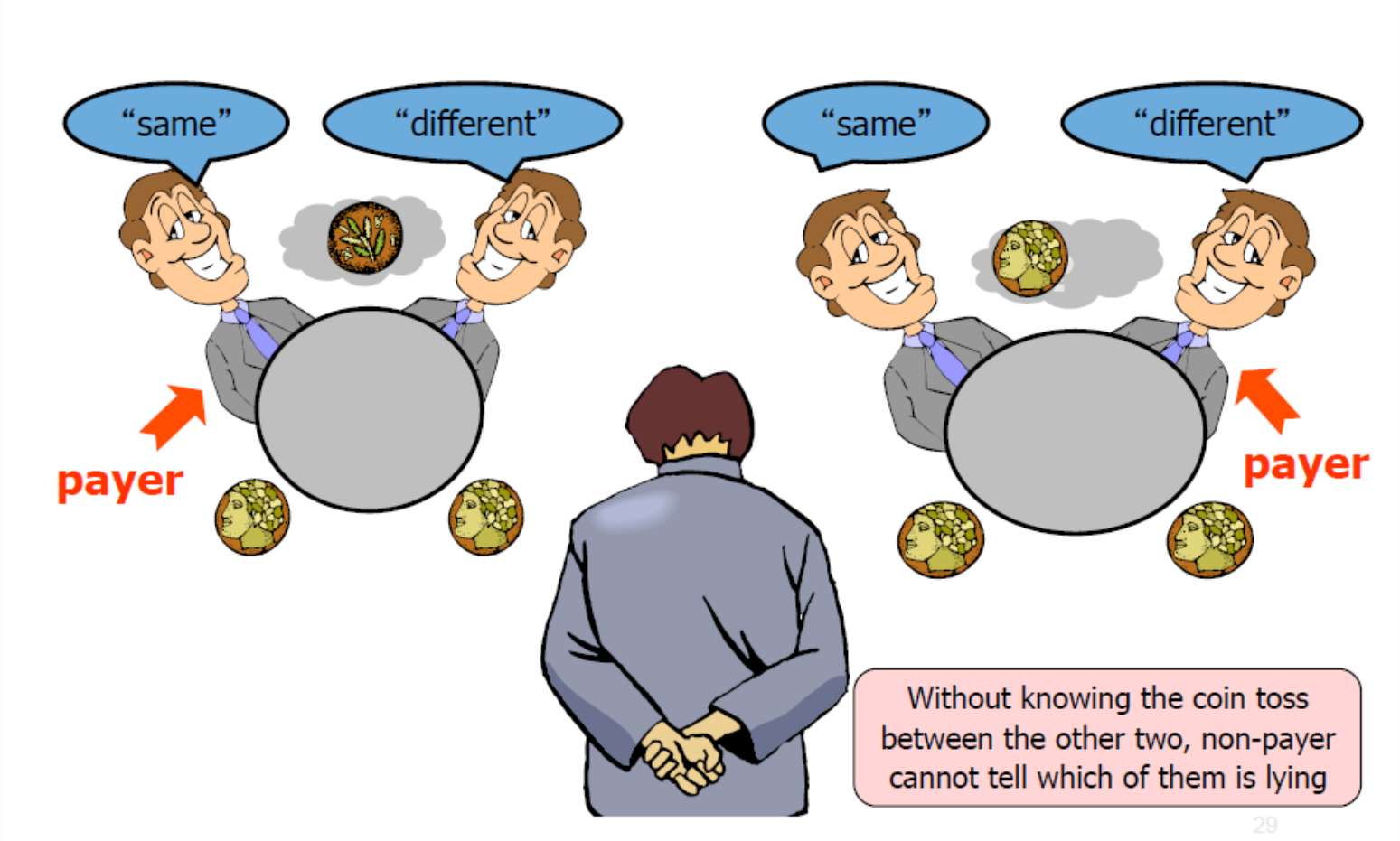
- *David Chaum. "The dining cryptographers problem: unconditional sender and recipient untraceability." Journal of Cryptology, 1988.*

Protocole

- Trois cryptographes sont en train de dîner.
- Soit la NSA paie le dîner ou alors l'un d'entre eux paie, mais souhaite rester anonyme.

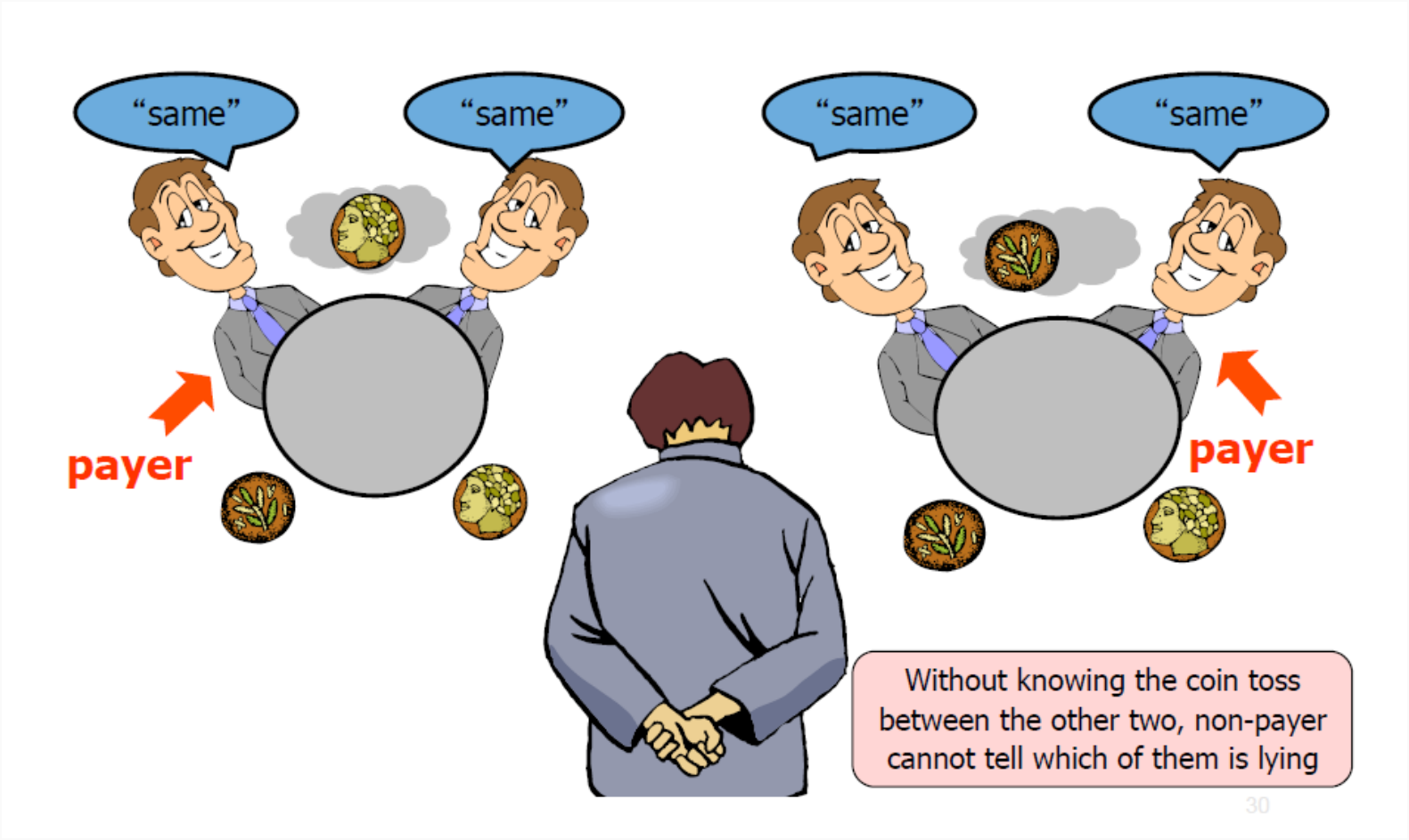
1. Chaque convive tire une pièce à pile ou face et montre le résultat à son voisin de gauche.
   - Chaque convive voit deux pièces : la sienne et celle de son voisin de droite.
2. Chaque convive annonce si les deux pièces sont identiques. S'il est le payeur, il ment (dit le contraire).
3. Résultat
   - un nombre impair de "identiques" alors la NSA a payé.
   - nombre pair de "identiques", l'un d'entre eux a payé. Mais un non-payeur ne peut pas savoir lequel des deux autres a payé.

Point de vue du non-payeur : “pièces identiques”



source http://sconce.ics.uci.edu/134-W18/slides/LEC15.pdf

Point de vue du non-payeur : “pièces différentes”



source http://sconce.ics.uci.edu/134-W18/slides/LEC15.pdf

Généralisation

Généralisation à un groupe de taille N

- Pour chaque bit du message, chaque utilisateur génère 1 bit aléatoire et l'envoie à 1 voisin
  - Chaque utilisateur connaît 2 bits (le sien et celui de son voisin)
- Chaque utilisateur annonce son propre bit XOR le bit du voisin
- L'expéditeur annonce son propre bit XOR le bit du voisin XOR le bit du message
- XOR de toutes les annonces = bit de message
  - Chaque bit généré aléatoirement apparaît deux fois dans cette somme (et est donc annulé par le XOR), le bit de message n'a qu'une seule occurrence.

Discussion

Les DC-Net ne sont pas réalistes

- Nécessite des canaux sécurisés par paires entre les membres du groupe
  - Sinon, les bits aléatoires ne peuvent pas être partagés de manière sûre
- Nécessite un important volume de communication ainsi qu'un très bon générateur aléatoire.
- Les DC-Net sont robustes même si certains membres sont de connivence
  - Garantit un anonymat parfait pour les autres membres