Anonymat en ligne: théorie et pratique (libre)

Laurent Fousse

Université Grenoble 1, CNRS, Laboratoire Jean Kuntzmann, France
Laurent.Fousse@imag.fr

GUILDE

13 octobre 2011

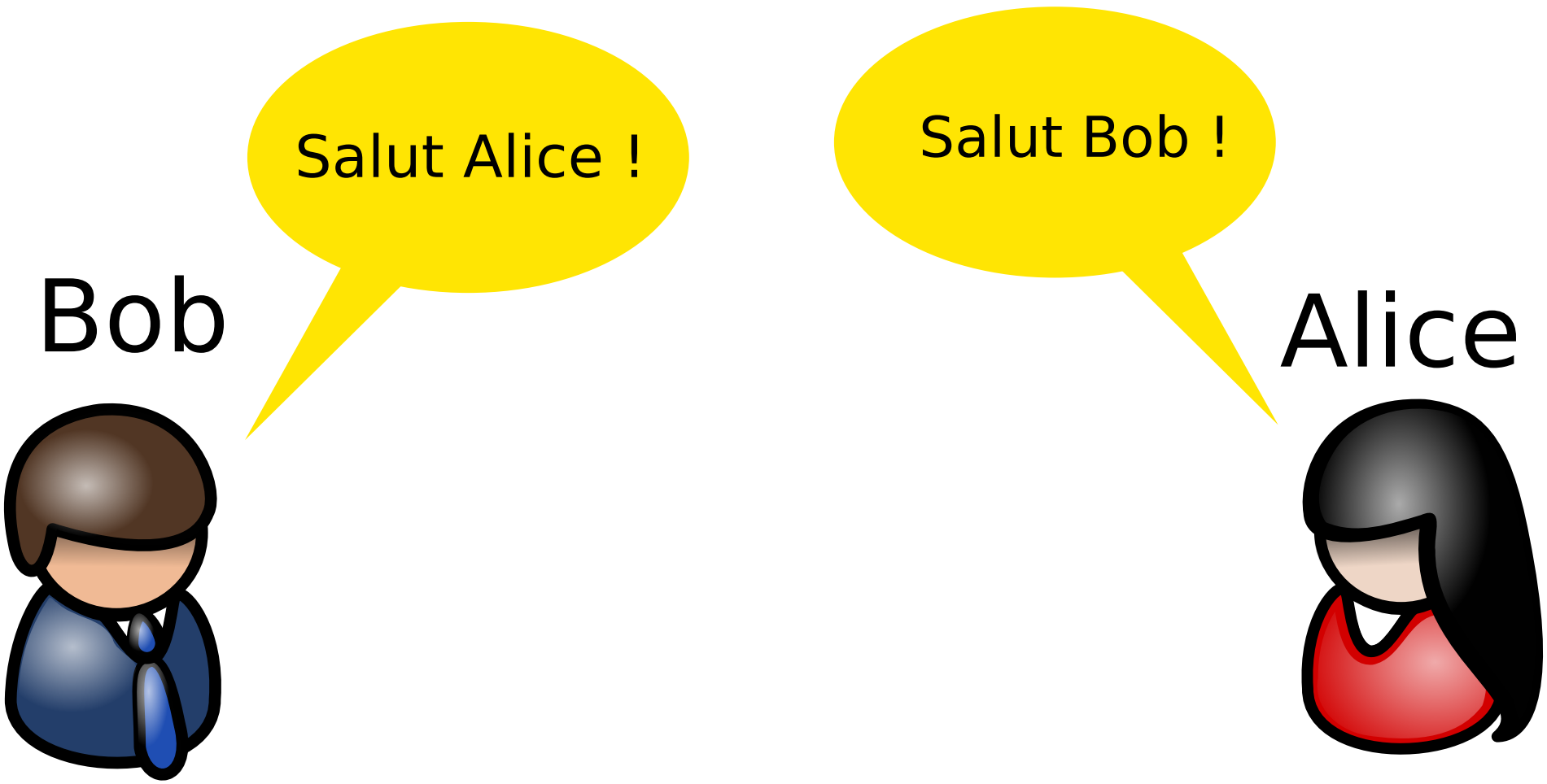
Plan

1. Anonymat ? (Quoi, pourquoi, pour qui...)
2. En théorie (ou comment produire de l'anonymat)
3. En pratique
4. Questions diverses
5. Conclusion

Plan

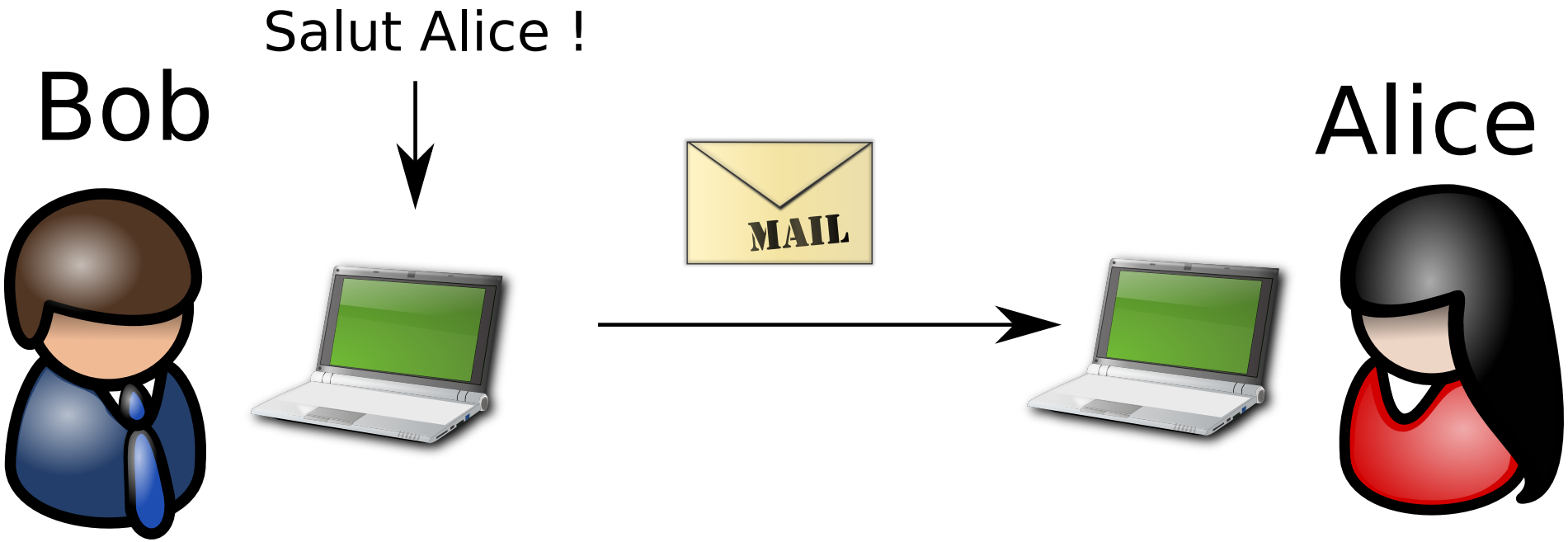
1. Anonymat ? (Quoi, pourquoi, pour qui...)
2. En théorie (ou comment produire de l'anonymat)
3. En pratique
4. Questions diverses
5. Conclusion

Problématique



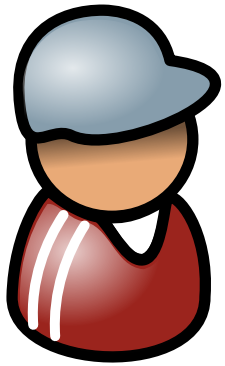
« Un petit quidam ça n'fait pas d'vague. »

Problématique



Problématique

Charlie



Bob

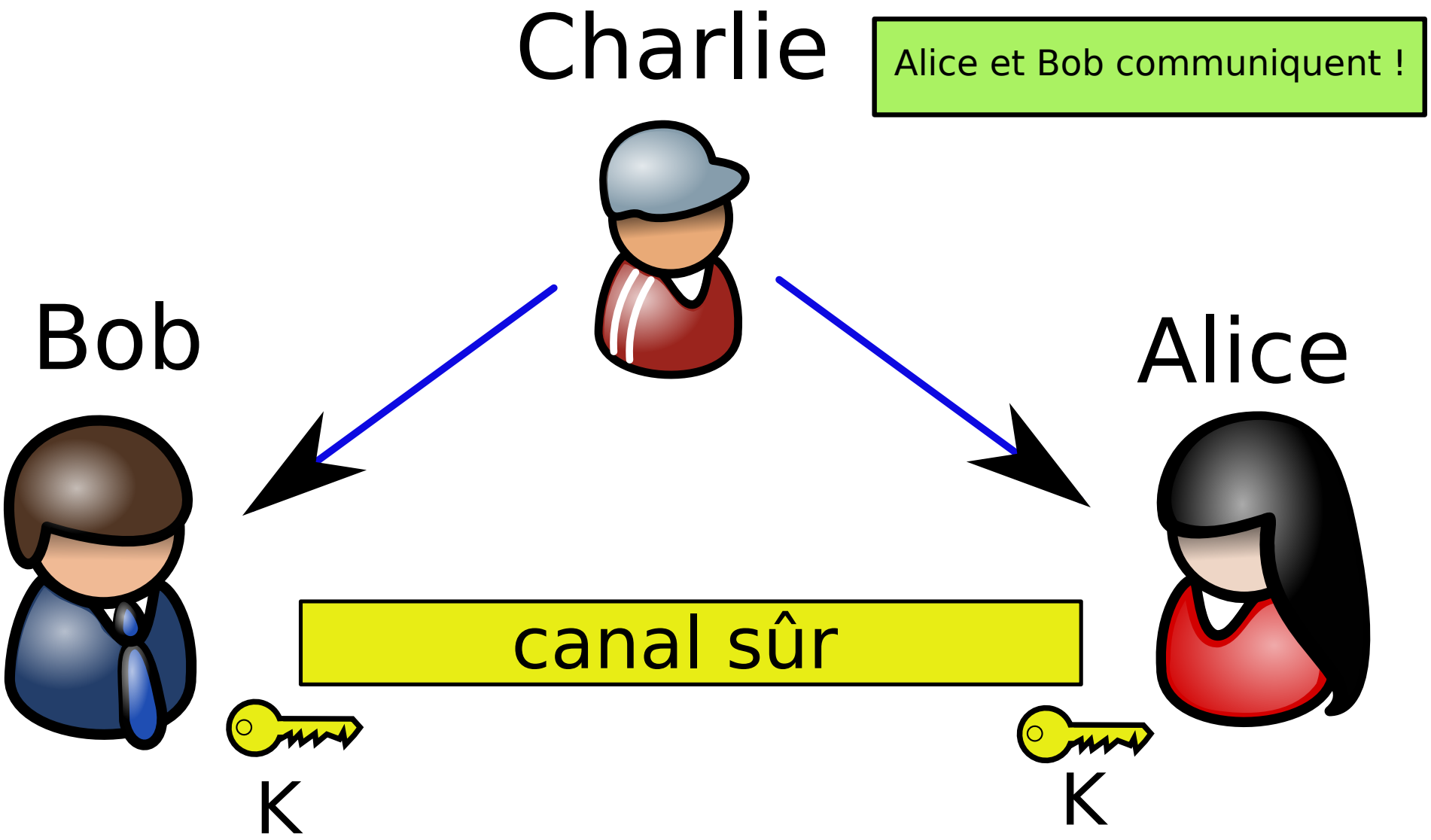
Alice

canal sûr

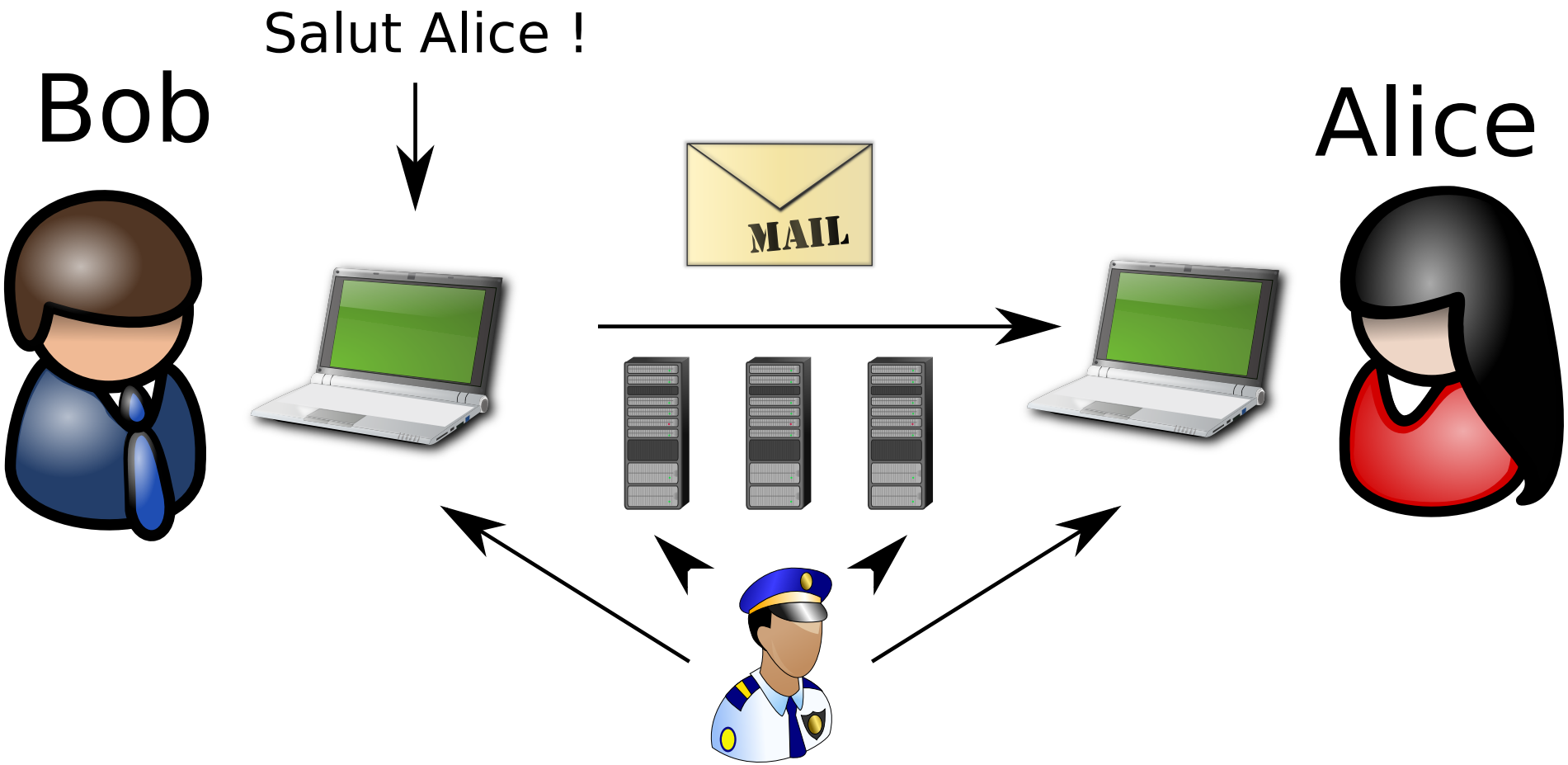
K

K

Problématique



Problématique



« Si tu n'as rien à cacher, tu n'as rien à craindre. »

Pour qui, pourquoi ?

Pourquoi ?

- Parce que toute activité en ligne laisse des traces :

Pour qui, pourquoi ?

Pourquoi ?

- Parce que toute activité en ligne laisse des traces :
- ... archivables sans limite de durée ;

Pour qui, pourquoi ?

Pourquoi ?

- Parce que toute activité en ligne laisse des traces :
- ... archivables sans limite de durée ;
- ... utilisables sans l'accord des personnes concernées ;

Pour qui, pourquoi ?

Pourquoi ?

- Parce que toute activité en ligne laisse des traces :
- ... archivables sans limite de durée ;
- ... utilisables sans l'accord des personnes concernées ;
- ... qui peuvent tomber entre n'importe quelles mains, surtout les pires ;

Pour qui, pourquoi ?

Pourquoi ?

- Parce que toute activité en ligne laisse des traces :
- ... archivables sans limite de durée ;
- ... utilisables sans l'accord des personnes concernées ;
- ... qui peuvent tomber entre n'importe quelles mains, surtout les pires ;
- Parce que le respect de la vie privée est un droit.

Pour qui, pourquoi ?

Pourquoi ?

- Parce que toute activité en ligne laisse des traces :
- ... archivables sans limite de durée ;
- ... utilisables sans l'accord des personnes concernées ;
- ... qui peuvent tomber entre n'importe quelles mains, surtout les pires ;
- Parce que le respect de la vie privée est un droit.
- Parce que les traces les plus faciles à effacer, c'est encore celles qu'on ne produit pas.

Pour qui, pourquoi ?

Pourquoi ?

- Parce que toute activité en ligne laisse des traces :
- ... archivables sans limite de durée ;
- ... utilisables sans l'accord des personnes concernées ;
- ... qui peuvent tomber entre n'importe quelles mains, surtout les pires ;
- Parce que le respect de la vie privée est un droit.
- Parce que les traces les plus faciles à effacer, c'est encore celles qu'on ne produit pas.
- Parce que le droit à l'oubli n'existe pas dans le monde numérique.

Pour qui, pourquoi ?

Pourquoi ?

- Parce que toute activité en ligne laisse des traces :
- ... archivables sans limite de durée ;
- ... utilisables sans l'accord des personnes concernées ;
- ... qui peuvent tomber entre n'importe quelles mains, surtout les pires ;
- Parce que le respect de la vie privée est un droit.
- Parce que les traces les plus faciles à effacer, c'est encore celles qu'on ne produit pas.
- Parce que le droit à l'oubli n'existe pas dans le monde numérique.
- Parce qu'il y a des circonstances où il est dangereux de *ne pas* être anonyme

Pour qui, pourquoi ?

Pourquoi ?

- Parce que toute activité en ligne laisse des traces :
- ... archivables sans limite de durée ;
- ... utilisables sans l'accord des personnes concernées ;
- ... qui peuvent tomber entre n'importe quelles mains, surtout les pires ;
- Parce que le respect de la vie privée est un droit.
- Parce que les traces les plus faciles à effacer, c'est encore celles qu'on ne produit pas.
- Parce que le droit à l'oubli n'existe pas dans le monde numérique.
- Parce qu'il y a des circonstances où il est dangereux de *ne pas* être anonyme
- $\rightarrow$ l'anonymat est un outil fondamental pour protéger sa vie privée en ligne.

Pour qui, pourquoi ?

Pour qui ?

- Pour le dissident chinois/iranien/*insérer ici le régime que vous jugez non démocratique de votre choix*.

Pour qui, pourquoi ?

Pour qui ?

- Pour le dissident chinois/iranien/*insérer ici le régime que vous jugez non démocratique de votre choix*.
- Pour voter en ligne (e.g. NetBSD).

Pour qui, pourquoi ?

Pour qui ?

- Pour le dissident chinois/iranien/*insérer ici le régime que vous jugez non démocratique de votre choix*.
- Pour voter en ligne (e.g. NetBSD).
- Pour payer en ligne (*anonymous e-cash*)

Pour qui, pourquoi ?

Pour qui ?

- Pour le dissident chinois/iranien/*insérer ici le régime que vous jugez non démocratique de votre choix*.
- Pour voter en ligne (e.g. NetBSD).
- Pour payer en ligne (*anonymous e-cash*)
- Pour l'indic interne à une entreprise, une administration, etc.

Pour qui, pourquoi ?

Pour qui ?

- Pour le dissident chinois/iranien/*insérer ici le régime que vous jugez non démocratique de votre choix*.
- Pour voter en ligne (e.g. NetBSD).
- Pour payer en ligne (*anonymous e-cash*)
- Pour l'indic interne à une entreprise, une administration, etc.
- Pour Madame Michu !

Pour qui, pourquoi ?

Pour qui ?

- Pour le dissident chinois/iranien/*insérer ici le régime que vous jugez non démocratique de votre choix*.
- Pour voter en ligne (e.g. NetBSD).
- Pour payer en ligne (*anonymous e-cash*)
- Pour l'indic interne à une entreprise, une administration, etc.
- Pour Madame Michu !

DUDH, Article 12

Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

Définition de l'anonymat

Anonymat

L'anonymat est la propriété de ne pas être identifiable parmi un ensemble de personnes appelé l'ensemble d'anonymat (*anonymity set*).

Définition de l'anonymat

Anonymat

L'anonymat est la propriété de ne pas être identifiable parmi un ensemble de personnes appelé l'ensemble d'anonymat (*anonymity set*).
$\rightarrow$ on n'est jamais anonyme tout seul...

Définition de l'anonymat

Anonymat

L'anonymat est la propriété de ne pas être identifiable parmi un ensemble de personnes appelé l'ensemble d'anonymat (*anonymity set*).
$\rightarrow$ on n'est jamais anonyme tout seul...

Définition probabiliste (entropie)

On est d'autant plus anonyme que l'ensemble d'anonymat est grand et que, dans cet ensemble, la probabilité que chacun soit la personne recherchée est distribué le plus uniformément possible.

Définition de l'anonymat

Anonymat

L'anonymat est la propriété de ne pas être identifiable parmi un ensemble de personnes appelé l'ensemble d'anonymat (*anonymity set*).
$\rightarrow$ on n'est jamais anonyme tout seul...

Définition probabiliste (entropie)

On est d'autant plus anonyme que l'ensemble d'anonymat est grand et que, dans cet ensemble, la probabilité que chacun soit la personne recherchée est distribué le plus uniformément possible.
$\rightarrow$ un géant est bien peu anonyme dans une assemblée de nains.

Définition de l'anonymat : cas des communications

Anonymat face à un tiers

Alice et Bob communiquent et se font confiance mais ne veulent pas qu'on le sache.

Définition de l'anonymat : cas des communications

Anonymat face à un tiers

Alice et Bob communiquent et se font confiance mais ne veulent pas qu'on le sache.

Anonymat de l'envoyeur

Alice envoie un message à Bob et personne, pas même Bob, ne doit savoir que cela vient d'Alice.

Définition de l'anonymat : cas des communications

Anonymat face à un tiers

Alice et Bob communiquent et se font confiance mais ne veulent pas qu'on le sache.

Anonymat de l'envoyeur

Alice envoie un message à Bob et personne, pas même Bob, ne doit savoir que cela vient d'Alice.

Anonymat du destinataire

Alice peut contacter Bob mais elle ne connaît pas sa véritable identité.

Définition de l'anonymat : cas des communications

Anonymat face à un tiers

Alice et Bob communiquent et se font confiance mais ne veulent pas qu'on le sache.

Anonymat de l'envoyeur

Alice envoie un message à Bob et personne, pas même Bob, ne doit savoir que cela vient d'Alice.

Anonymat du destinataire

Alice peut contacter Bob mais elle ne connaît pas sa véritable identité.

Anonymat bidirectionnelle

Alice et Bob communiquent sans connaître l'identité l'un de l'autre.

Anonymat vs. confidentialité des données

Zéro protection	Alice cherche “Dennis Ritchie” sur le web
Anonymat	*Quelqu’un* cherche “Dennis Ritchie” sur le web
Confidentialité	Alice cherche *quelque chose* sur le web

Anonymat vs. confidentialité des données

Zéro protection	Alice cherche “Dennis Ritchie” sur le web
Anonymat	*Quelqu’un* cherche “Dennis Ritchie” sur le web
Confidentialité	Alice cherche *quelque chose* sur le web

Zéro protection	Alice consulte sa boîte mél `lulu@example.net`
Anonymat	*Quelqu’un* consulte sa boîte mél `lulu@example.net`
Confidentialité	Alice consulte une boîte mél du serveur `example.net`.

Anonymat vs. confidentialité des données

Zéro protection	Alice cherche “Dennis Ritchie” sur le web
Anonymat	*Quelqu’un* cherche “Dennis Ritchie” sur le web
Confidentialité	Alice cherche *quelque chose* sur le web

Zéro protection	Alice consulte sa boîte mél `lulu@example.net`
Anonymat	*Quelqu’un* consulte sa boîte mél `lulu@example.net`
Confidentialité	Alice consulte une boîte mél du serveur `example.net`.

Définition/Rappel

- Il y a anonymat lorsque le serveur observe l’accès, pas l’identité.
- Il y a confidentialité lorsque le serveur observe l’identité, pas la requête.
- On peut espérer combiner les deux.

Plan

1. Anonymat ? (Quoi, pourquoi, pour qui...)
2. En théorie (ou comment produire de l'anonymat)
3. En pratique
4. Questions diverses
5. Conclusion

Mix network

Monde analogique

1. Alice prépare sa lettre à Bob, qu'elle affranchit sans signer la lettre ni marquer l'enveloppe.

Monde analogique

1. Alice prépare sa lettre à Bob, qu'elle affranchit sans signer la lettre ni marquer l'enveloppe.
2. Elle place sa lettre pour Bob dans une enveloppe qu'elle adresse à Charlie.

Mix network

Monde analogique

1. Alice prépare sa lettre à Bob, qu'elle affranchit sans signer la lettre ni marquer l'enveloppe.
2. Elle place sa lettre pour Bob dans une enveloppe qu'elle adresse à Charlie.
3. Charlie ouvre son courrier, sort l'enveloppe pour Bob qu'il poste à son tour.

Monde analogique

1. Alice prépare sa lettre à Bob, qu'elle affranchit sans signer la lettre ni marquer l'enveloppe.
2. Elle place sa lettre pour Bob dans une enveloppe qu'elle adresse à Charlie.
3. Charlie ouvre son courrier, sort l'enveloppe pour Bob qu'il poste à son tour.
4. Bob reçoit un courrier non marqué, non signé, provenant de Houte-Si-Plou (commune de Charlie) où il ne connaît personne !

Mix network

Monde analogique

1. Alice prépare sa lettre à Bob, qu'elle affranchit sans signer la lettre ni marquer l'enveloppe.
2. Elle place sa lettre pour Bob dans une enveloppe qu'elle adresse à Charlie.
3. Charlie ouvre son courrier, sort l'enveloppe pour Bob qu'il poste à son tour.
4. Bob reçoit un courrier non marqué, non signé, provenant de Houte-Si-Plou (commune de Charlie) où il ne connaît personne !

Analyse

- L'anonymat d'Alice dépend de la complicité de Charlie.

Mix network

Monde analogique

1. Alice prépare sa lettre à Bob, qu'elle affranchit sans signer la lettre ni marquer l'enveloppe.
2. Elle place sa lettre pour Bob dans une enveloppe qu'elle adresse à Charlie.
3. Charlie ouvre son courrier, sort l'enveloppe pour Bob qu'il poste à son tour.
4. Bob reçoit un courrier non marqué, non signé, provenant de Houte-Si-Plou (commune de Charlie) où il ne connaît personne !

Analyse

- L'anonymat d'Alice dépend de la complicité de Charlie.
- On peut augmenter le nombre de maillons (il suffit que l'un d'eux soit « honnête »).

Mix network

Monde analogique

1. Alice prépare sa lettre à Bob, qu'elle affranchit sans signer la lettre ni marquer l'enveloppe.
2. Elle place sa lettre pour Bob dans une enveloppe qu'elle adresse à Charlie.
3. Charlie ouvre son courrier, sort l'enveloppe pour Bob qu'il poste à son tour.
4. Bob reçoit un courrier non marqué, non signé, provenant de Houte-Si-Plou (commune de Charlie) où il ne connaît personne !

Analyse

- L'anonymat d'Alice dépend de la complicité de Charlie.
- On peut augmenter le nombre de maillons (il suffit que l'un d'eux soit « honnête »).
- L'intégrité du service postal est cruciale.

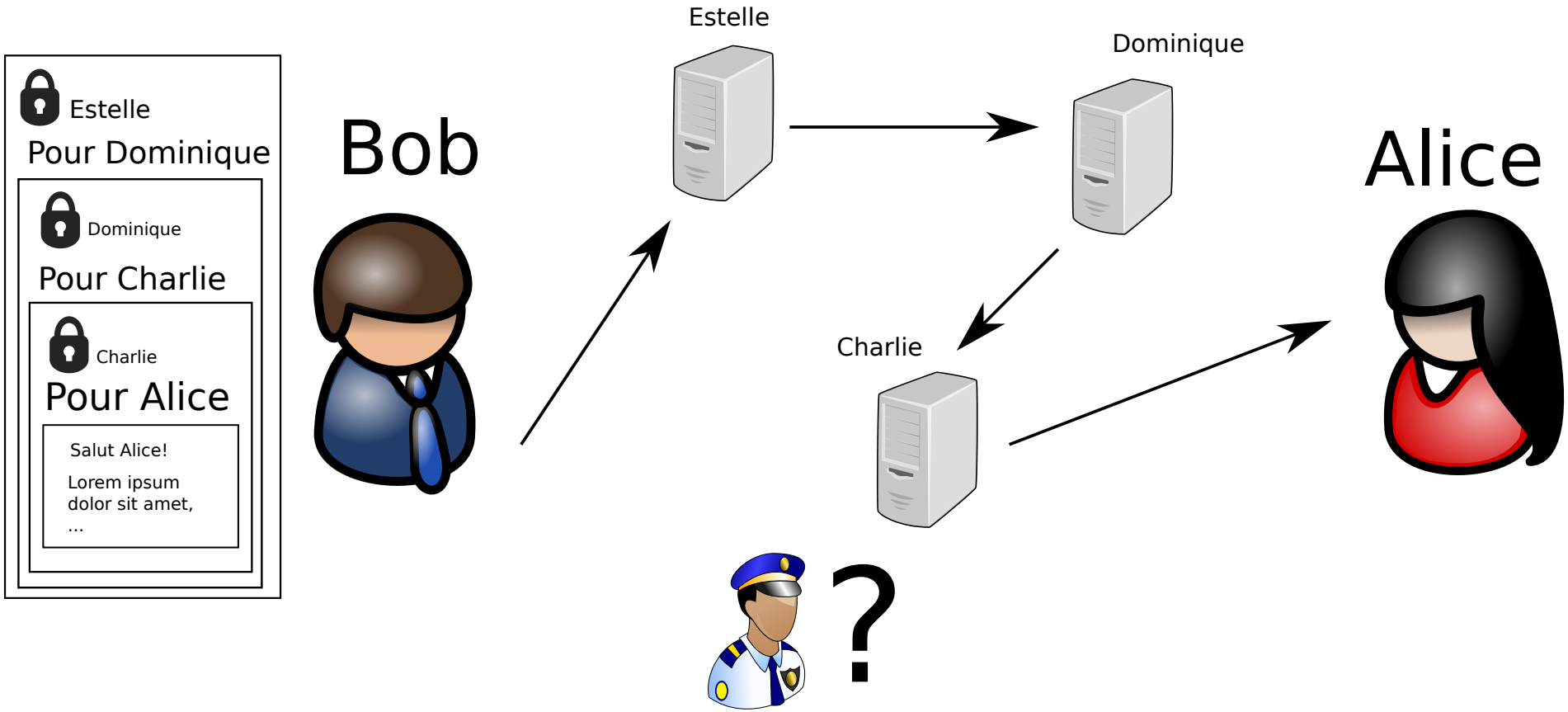
Mix network

David Chaum, 1981

Adaptation numérique du protocole précédent :

Analogique	Numérique
Service postal	Couche “transport” (`http`, `smtp`, ...)
Enveloppe	Chiffrement à clef publique
Complices humains	Complices *humains* et leurs machines

Mix network


Estelle
Pour Dominique
Dominique
Pour Charlie
Charlie
Pour Alice
Salut Alice!
Lorem ipsum
dolor sit amet,
...
Bob
Estelle
Dominique
Charlie
Alice
?

Mix network

Point de vue mathématique

- n complices dotés chacun d'une bi-clef publique-privée (K_i, K_i').
- Pour envoyer un message m, Bob choisit k complices parmi les n et calcule
$$c_0 = E_{K_{i_0}}(E_{K_{i_1}}(\ldots E_{K_{i_k}}(m))\ldots).$$
- le complice numéro i reçoit le message c_i et calcule $c_{i+1} = D_{K_i'}(c_i)$ qu'il envoie au suivant.
- Alice reçoit $c_k = m$ du dernier complice.
- Il suffit qu'un complice soit honnête pour perdre le lien entre c_i et c_{i+1} et garantir l'anonymat de Bob (sous certaines hypothèses).

Mix network

Point de vue mathématique

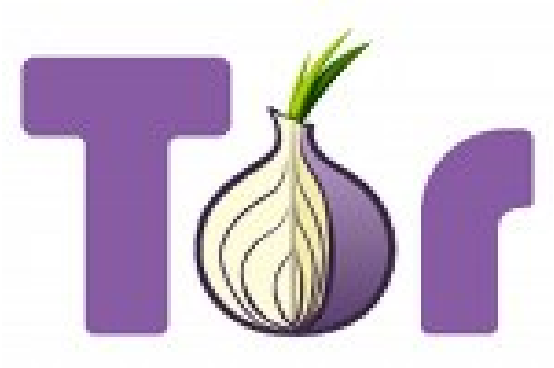
- n complices dotés chacun d'une bi-clef publique-privée (K_i, K_i').
- Pour envoyer un message m, Bob choisit k complices parmi les n et calcule
$$c_0 = E_{K_{i_0}}(E_{K_{i_1}}(\ldots E_{K_{i_k}}(m))\ldots).$$
- le complice numéro i reçoit le message c_i et calcule $c_{i+1} = D_{K_i'}(c_i)$ qu'il envoie au suivant.
- Alice reçoit $c_k = m$ du dernier complice.
- Il suffit qu'un complice soit honnête pour perdre le lien entre c_i et c_{i+1} et garantir l'anonymat de Bob (sous certaines hypothèses).

On comprend pourquoi on parle de *routage en oignon* : chaque complice dans la chaîne « épluche » une pelure (techniquement : déchiffre un niveau de chiffrement) pour découvrir la destination suivante et le message à lui transmettre.

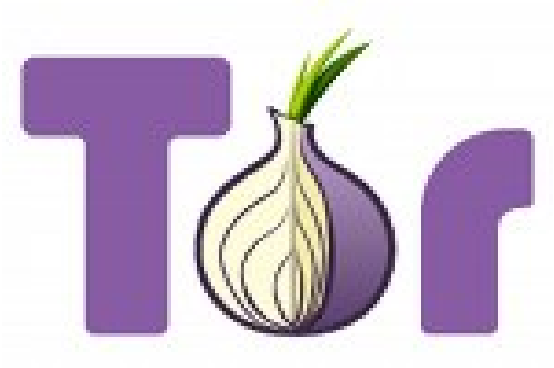
Plan

1. Anonymat ? (Quoi, pourquoi, pour qui...)
2. En théorie (ou comment produire de l'anonymat)
3. En pratique
4. Questions diverses
5. Conclusion

Navigation web : Tor



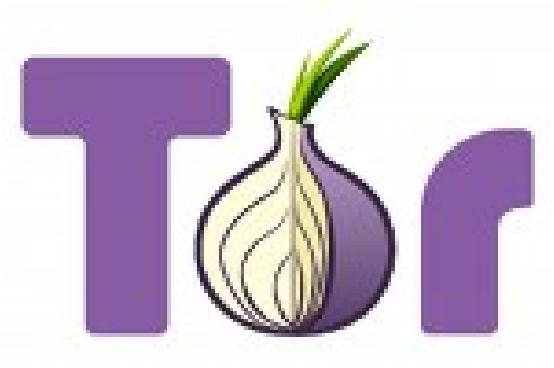
Navigation web : Tor



TCP Onion Routing

- Logiciel *libre* (BSD) ;

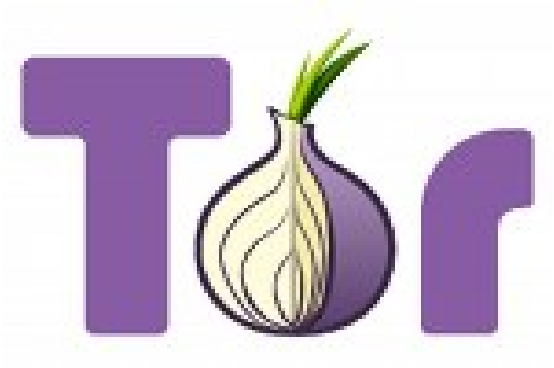
Navigation web : Tor



TCP Onion Routing

- Logiciel *libre* (BSD) ;
- Nœuds Tor composant le réseau ;

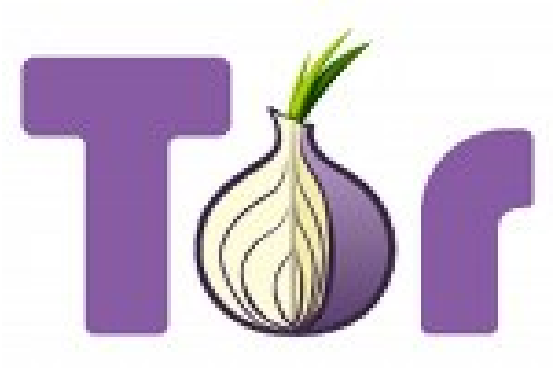
Navigation web : Tor



TCP Onion Routing

- Logiciel *libre* (BSD) ;
- Nœuds Tor composant le réseau ;
- Client permettant d'encapsuler du trafic TCP dans le réseau Tor ;

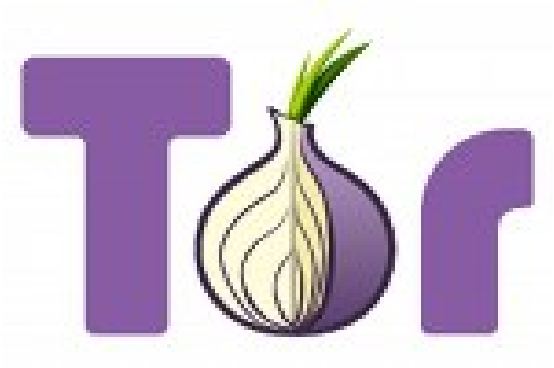
Navigation web : Tor



TCP Onion Routing

- Logiciel *libre* (BSD) ;
- Nœuds Tor composant le réseau ;
- Client permettant d'encapsuler du trafic TCP dans le réseau Tor ;
- Le chemin (*circuit*) est construit incrémentalement par le client pour transmettre du contenu (*cell*) dans les deux directions ;

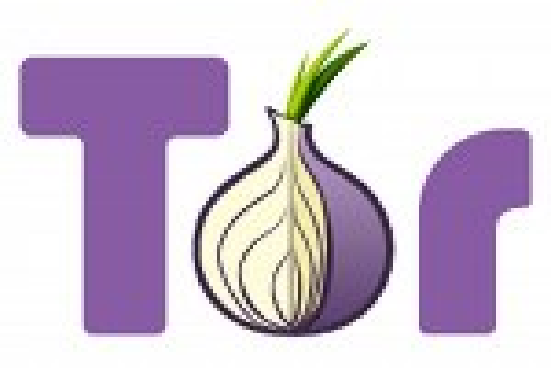
Navigation web : Tor



TCP Onion Routing

- Logiciel *libre* (BSD) ;
- Nœuds Tor composant le réseau ;
- Client permettant d'encapsuler du trafic TCP dans le réseau Tor ;
- Le chemin (*circuit*) est construit incrémentalement par le client pour transmettre du contenu (*cell*) dans les deux directions ;
- Permet l'anonymat bi-directionnel (*hidden-service*) ;

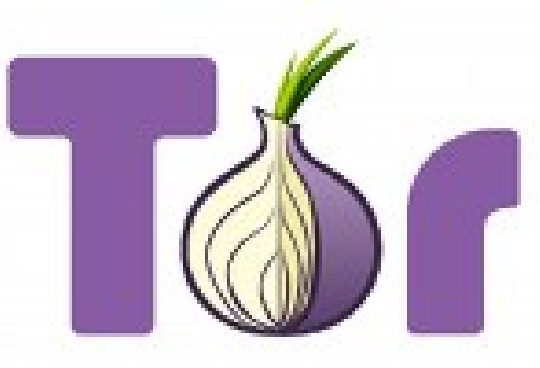
Navigation web : Tor



TCP Onion Routing

- Logiciel *libre* (BSD) ;
- Nœuds Tor composant le réseau ;
- Client permettant d'encapsuler du trafic TCP dans le réseau Tor ;
- Le chemin (*circuit*) est construit incrémentalement par le client pour transmettre du contenu (*cell*) dans les deux directions ;
- Permet l'anonymat bi-directionnel (*hidden-service*) ;
- Vise à protéger contre des attaquants très puissants (vue $\pm$ globale du réseau) ;

Navigation web : Tor

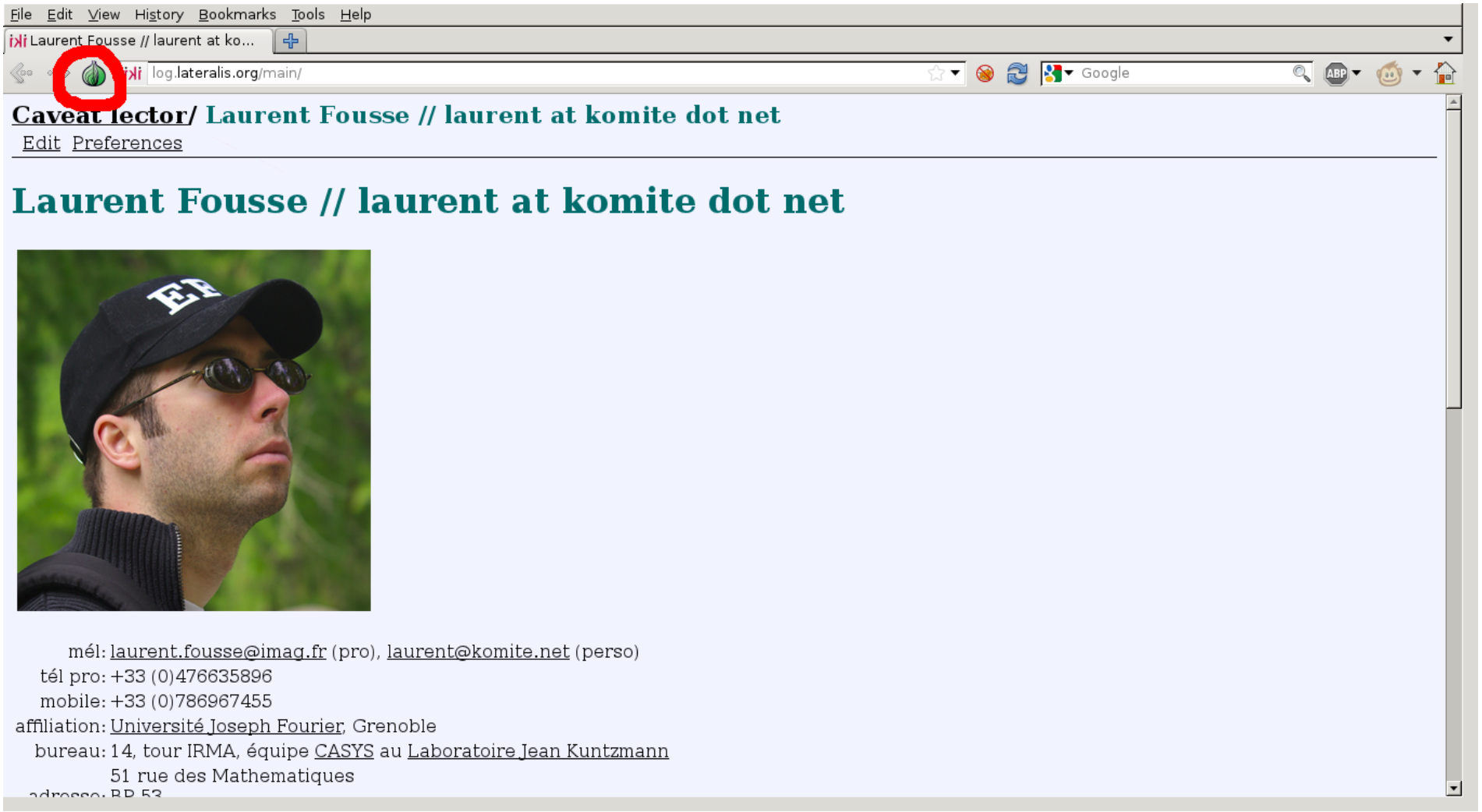


TCP Onion Routing

- Logiciel *libre* (BSD) ;
- Nœuds Tor composant le réseau ;
- Client permettant d'encapsuler du trafic TCP dans le réseau Tor ;
- Le chemin (*circuit*) est construit incrémentalement par le client pour transmettre du contenu (*cell*) dans les deux directions ;
- Permet l'anonymat bi-directionnel (*hidden-service*) ;
- Vise à protéger contre des attaquants très puissants (vue $\pm$ globale du réseau) ;
- Divers logiciels tiers (Torbutton, ...).

Torbutton

```
# apt-get install tor
```



Envoi de courriel : Mixmaster

Présentation

- Logiciel *libre* (licence *ad-hoc*)

Envoi de courriel : Mixmaster

Présentation

- Logiciel *libre* (licence *ad-hoc*)
- Application des *mixnets* au courriel.

Envoi de courriel : Mixmaster

Présentation

- Logiciel *libre* (licence *ad-hoc*)
- Application des *mixnets* au courriel.
- Grande latence.

Envoi de courriel : Mixmaster

Présentation

- Logiciel *libre* (licence *ad-hoc*)
- Application des *mixnets* au courriel.
- Grande latence.
- Trafic factice injecté par les nœuds du réseau.

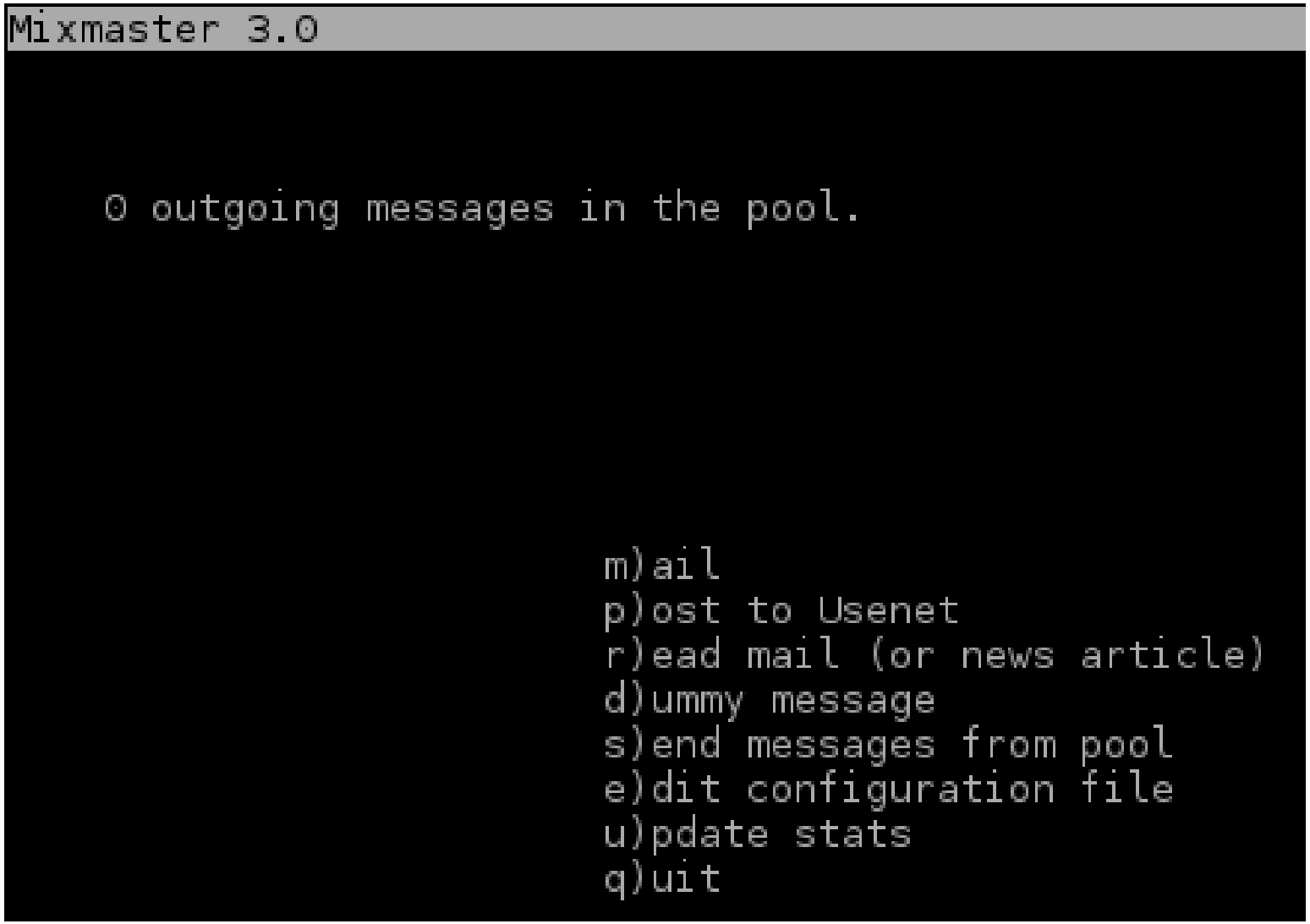
Envoi de courriel : Mixmaster

Présentation

- Logiciel *libre* (licence *ad-hoc*)
- Application des *mixnets* au courriel.
- Grande latence.
- Trafic factice injecté par les nœuds du réseau.
- Courriels réexpédiés dans un ordre aléatoire.

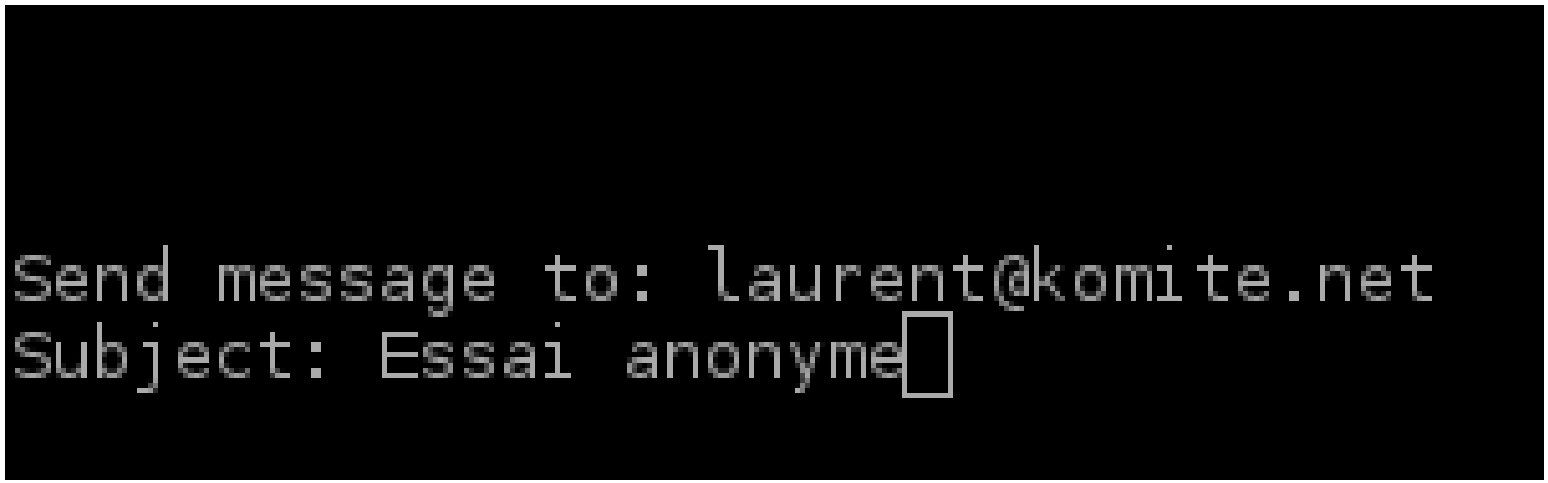
Envoi de courriel : Mixmaster

Menu principal



Envoi de courriel : Mixmaster

Préparation d'un message



Envoi de courriel : Mixmaster

Rédaction d'un message

```
To: laurent@komite.net
Subject: Essai anonyme

Exemple de courriel anonyme.

Laurent.

PS: oups, je voulais pas vraiment signer.
~
```

Envoi de courriel : Mixmaster

Envoi d'un message

```
Mixmaster 3.0 - sending mail



c)hain: *,*,*,*                                  (reliability:   n/a  )
r)edundancy:    1 copies

d)estination: laurent@komite.net
s)ubject: Essai anonyme

pgp encry)ption: no
```

Envoi de courriel : Mixmaster

Via mutt

```
y:Send  q:Abort  t:To  c:CC  s:Subj  a:Attach file  d:Descrip  ?:Help
    From: Laurent Fousse <laurent@komite.net>
      To: Laurent Fousse <laurent@komite.net>
      Cc:
     Bcc:
 Subject: Mixmaster via mutt
Reply-To:
     Fcc: ~/sent
     Mix: banana, kroken, lulunga, *
Security: Clear

-- Attachments
- I     1 /tmp/mutt-purple-1000-11764-11925f325c98



-- Mutt: Compose  [Approx. msg size: 0.1K   Atts: 1]----------------------
```

Envoi de courriel : Mixmaster

À la réception :

```
From: Fritz Wuehler
<fritz@spamexpire-201110.rodent.frell.theremailer.net>
To: laurent@komite.net
Subject: Essai 2
```

Plan

1. Anonymat ? (Quoi, pourquoi, pour qui...)
2. En théorie (ou comment produire de l'anonymat)
3. En pratique
4. Questions diverses
5. Conclusion

Anonymat : les bons

Les amis de l'anonymat

- le nombre ;

Anonymat : les bons

Les amis de l'anonymat

- le nombre ;
- l'utilisabilité ;

Anonymat : les bons

Les amis de l'anonymat

- le nombre ;
- l'utilisabilité ;
- les spammeurs (!)

Anonymat : les bons

Les amis de l'anonymat

- le nombre ;
- l'utilisabilité ;
- les spammeurs (!)
- la latence ;

Anonymat : les bons

Les amis de l'anonymat

- le nombre ;
- l'utilisabilité ;
- les spammeurs (!)
- la latence ;
- les opérateurs de nœuds (tor, mixmaster) ;

Anonymat : les bons

Les amis de l'anonymat

- le nombre ;
- l'utilisabilité ;
- les spammeurs (!)
- la latence ;
- les opérateurs de nœuds (tor, mixmaster) ;
- les développeurs de logiciels qui maîtrisent la problématique ;

Anonymat : les bons

Les amis de l'anonymat

- le nombre ;
- l'utilisabilité ;
- les spammeurs (!)
- la latence ;
- les opérateurs de nœuds (tor, mixmaster) ;
- les développeurs de logiciels qui maîtrisent la problématique ;
- l'EFF.

Anonymat : les truands

Il ne faut pas oublier

- l'anonymat produit se limite à la couche réseau (aucune protection « sémantique ») ;

Anonymat : les truands

Il ne faut pas oublier

- l'anonymat produit se limite à la couche réseau (aucune protection « sémantique ») ;
- un *mixnet* ne fournit pas de chiffrement de bout en bout (cf. attaque équipe INRIA Planète).

Anonymat : les truands

Il ne faut pas oublier

- l'anonymat produit se limite à la couche réseau (aucune protection « sémantique ») ;
- un *mixnet* ne fournit pas de chiffrement de bout en bout (cf. attaque équipe INRIA Planète).
- $\rightarrow$ attention au faux sentiment de sécurité !

Anonymat : les brutes

Les ennemis de l'anonymat

- les *bugs* logiciels

Anonymat : les brutes

Les ennemis de l'anonymat

- les *bugs* logiciels
- les systèmes d'exploitation douteux ;

Anonymat : les brutes

Les ennemis de l'anonymat

- les *bugs* logiciels
- les systèmes d'exploitation douteux ;
- les applications clientes (le navigateur, le logiciel de courriel)

Anonymat : les brutes

Les ennemis de l'anonymat

- les *bugs* logiciels
- les systèmes d'exploitation douteux ;
- les applications clientes (le navigateur, le logiciel de courriel) $\rightarrow$ étude Panopticlick de l'EFF.

Anonymat : les brutes

Les ennemis de l'anonymat

- les *bugs* logiciels
- les systèmes d'exploitation douteux ;
- les applications clientes (le navigateur, le logiciel de courriel) $\rightarrow$ étude Panopticlick de l'EFF.
- les intimidations policières.

Anonymat : les brutes

Les ennemis de l'anonymat

- les *bugs* logiciels
- les systèmes d'exploitation douteux ;
- les applications clientes (le navigateur, le logiciel de courriel) $\rightarrow$ étude Panopticlick de l'EFF.
- les intimidations policières.
- l'utilisateur !

Tout ceci est-il bien légal ?

- Est-il légal (en France) de chercher à procurer de l'anonymat ?
- Est-il légal (en France) de chercher à agir sous couvert de l'anonymat ?

Plan

1. Anonymat ? (Quoi, pourquoi, pour qui...)
2. En théorie (ou comment produire de l'anonymat)
3. En pratique
4. Questions diverses
5. Conclusion

En résumé

- l'anonymat est un outil dans une démarche globale de protection de la sphère privée ;

En résumé

- l'anonymat est un outil dans une démarche globale de protection de la sphère privée ;
- l'anonymat est une notion probabiliste ;

En résumé

- l'anonymat est un outil dans une démarche globale de protection de la sphère privée ;
- l'anonymat est une notion probabiliste ;
- il existe des solutions théoriques plus ou moins satisfaisantes ;

En résumé

- l'anonymat est un outil dans une démarche globale de protection de la sphère privée ;
- l'anonymat est une notion probabiliste ;
- il existe des solutions théoriques plus ou moins satisfaisantes ;
- et des attaques possibles ;

En résumé

- l'anonymat est un outil dans une démarche globale de protection de la sphère privée ;
- l'anonymat est une notion probabiliste ;
- il existe des solutions théoriques plus ou moins satisfaisantes ;
- et des attaques possibles ;
- il existe des implémentations libres ;

En résumé

- l'anonymat est un outil dans une démarche globale de protection de la sphère privée ;
- l'anonymat est une notion probabiliste ;
- il existe des solutions théoriques plus ou moins satisfaisantes ;
- et des attaques possibles ;
- il existe des implémentations libres ;
- et des attaques sur ces implémentations !

En résumé

- l'anonymat est un outil dans une démarche globale de protection de la sphère privée ;
- l'anonymat est une notion probabiliste ;
- il existe des solutions théoriques plus ou moins satisfaisantes ;
- et des attaques possibles ;
- il existe des implémentations libres ;
- et des attaques sur ces implémentations !
- l'approche de la confidentialité des requêtes est peu implémenté ;

En résumé

- l'anonymat est un outil dans une démarche globale de protection de la sphère privée ;
- l'anonymat est une notion probabiliste ;
- il existe des solutions théoriques plus ou moins satisfaisantes ;
- et des attaques possibles ;
- il existe des implémentations libres ;
- et des attaques sur ces implémentations !
- l'approche de la confidentialité des requêtes est peu implémenté ;
- on ne choisit pas à qui on fournit de l'anonymat ! (démarche militante)

En résumé

- l'anonymat est un outil dans une démarche globale de protection de la sphère privée ;
- l'anonymat est une notion probabiliste ;
- il existe des solutions théoriques plus ou moins satisfaisantes ;
- et des attaques possibles ;
- il existe des implémentations libres ;
- et des attaques sur ces implémentations !
- l'approche de la confidentialité des requêtes est peu implémenté ;
- on ne choisit pas à qui on fournit de l'anonymat ! (démarche militante)
- malgré les "scandales" répétés, l'utilisateur est peu conscient/intéressé par la problématique ;

En résumé

- l'anonymat est un outil dans une démarche globale de protection de la sphère privée ;
- l'anonymat est une notion probabiliste ;
- il existe des solutions théoriques plus ou moins satisfaisantes ;
- et des attaques possibles ;
- il existe des implémentations libres ;
- et des attaques sur ces implémentations !
- l'approche de la confidentialité des requêtes est peu implémenté ;
- on ne choisit pas à qui on fournit de l'anonymat ! (démarche militante)
- malgré les "scandales" répétés, l'utilisateur est peu conscient/intéressé par la problématique ;
- l'anonymat a un coût (calculatoire, en latence).