# Automated Verification of Privacy in Security Protocols: Back and Forth Between Theory & Practice

## Journées Nationales 2018 du Pré-GDR Sécurité Informatique

Lucca Hirschi

Thèse encadrée par David Baelde et Stéphanie Delaune

ETH zürich

31 mai 2018

# Concevoir des protocoles cryptographiques sûrs

TLS


Complexité du problème

- réseau non sécurisé
- attaquant actif
- exécutions concurrentes

# Concevoir des protocoles cryptographiques sûrs

**Accessibilité** (ex. authentification)

TLS


modèles 80's

algos/outils

00's

maturité industrielle

2018

Complexité du problème

- réseau non sécurisé
- attaquant actif
- exécutions concurrentes

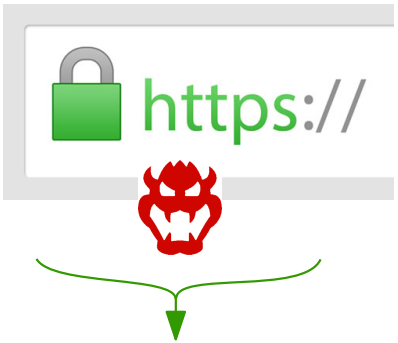
Méthodes formelles & modèle symbolique

- analyses mathématiques & exhaustives
- garanties formelles
- automatisé ou automatique

# Concevoir des protocoles cryptographiques sûrs

**Accessibilité** (ex. authentification)

TLS




Standard TLS 1.3 muni de garanties formelles

modèles 80's

algos/outils 00's

maturité industrielle 2018

Complexité du problème

- réseau non sécurisé
- attaquant actif
- exécutions concurrentes

Méthodes formelles & modèle symbolique

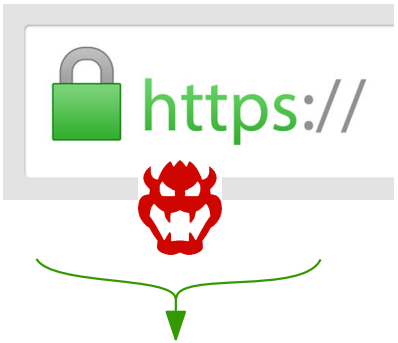
- analyses mathématiques & exhaustives
- garanties formelles
- automatisé ou automatique

# Concevoir des protocoles cryptographiques sûrs

**Accessibilité** (ex. authentification)

**Equivalence**: **privacy** (ex. intraçabilité)

TLS




Standard TLS 1.3 muni de garanties formelles

modèles 80's

algos/outils

00's modèles

algos/outils

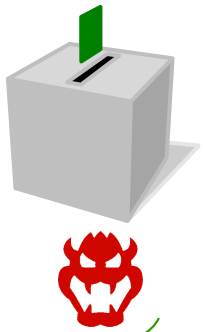
maturité industrielle

2018

maturité industrielle ?

Mobilité (5G)

E-Voting



Défis scientifiques

Complexité du problème

- réseau non sécurisé
- attaquant actif
- exécutions concurrentes

Méthodes formelles & modèle symbolique

- analyses mathématiques & exhaustives
- garanties formelles
- automatisé ou automatique

# Vérification symbolique de privacy – État de l'art

modèles de protocoles (ex. applied $\pi$-calculus)

Problème: $\forall A_{\text{😈}}, \; P|A_{\text{😈}} \approx Q|A_{\text{😈}}$

équivalence observationnelle

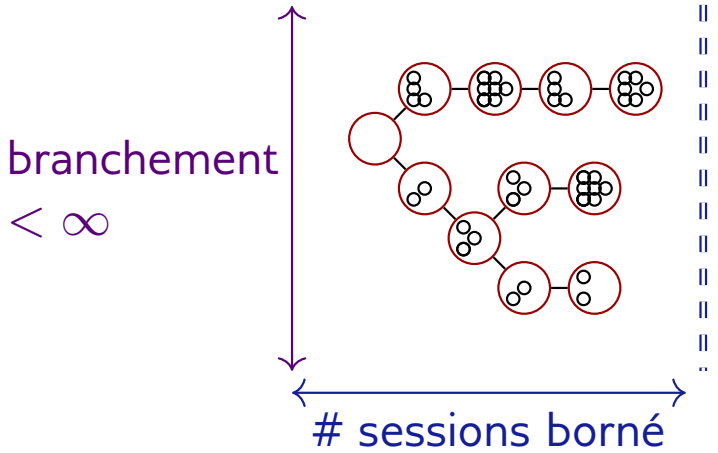
# Vérification symbolique de privacy – État de l'art

modèles de protocoles (ex. applied $\pi$-calculus)

Problème: $\forall A_{\text{😈}},\ P|A_{\text{😈}} \approx Q|A_{\text{😈}}$

équivalence observationnelle

## Décision pour $< \infty$ sessions




- borner le nombre de sessions
- sémantique symbolique
- exploration exhaustive des exécutions symboliques
- Outils: DeepSec, Apte, Akiss, Spec

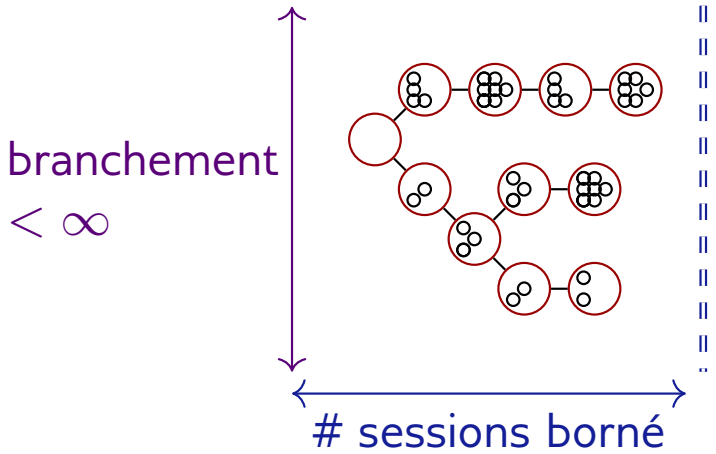
# Vérification symbolique de privacy – État de l'art

modèles de protocoles (ex. applied $\pi$-calculus)

Problème: $\forall A_{\text{😈}}, \; P|A_{\text{😈}} \approx Q|A_{\text{😈}}$

équivalence observationnelle

## Décision pour $< \infty$ sessions




- borner le nombre de sessions
- sémantique symbolique
- exploration exhaustive des exécutions symboliques
- Outils: **Explosion # états**

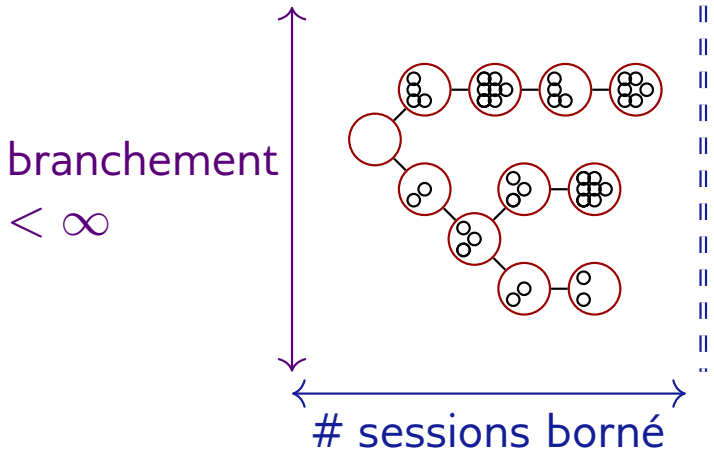
# Vérification symbolique de privacy – État de l'art

modèles de protocoles (ex. applied $\pi$-calculus)

Problème: $\forall A_{\text{🐢}}, P|A_{\text{🐢}} \approx Q|A_{\text{🐢}}$

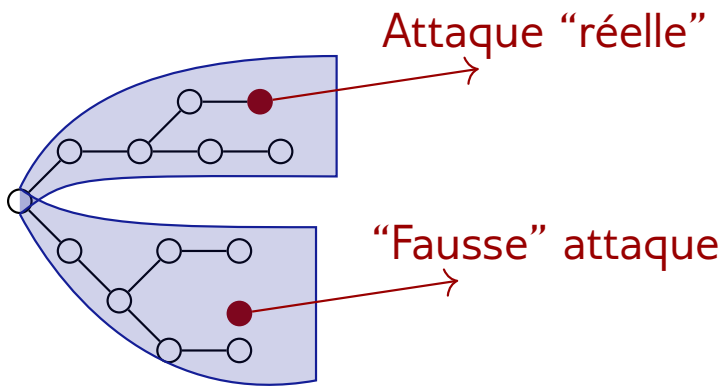
équivalence observationnelle

## Décision pour $< \infty$ sessions




- borner le nombre de sessions
- sémantique symbolique
- exploration exhaustive des exécutions symboliques
- Outils: Explosion # états

## Semi-décision pour $\infty$ sessions




- sur-approximations de l'🐢 & la sémantique
- forme forte d'$\approx$ (*i.e.* diff-equivalence)
- Outils: ProVerif, Tamarin, Maude-NPA

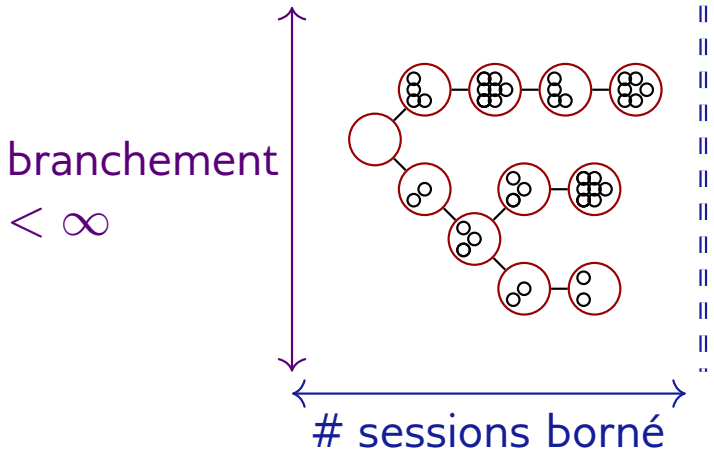
# Vérification symbolique de privacy – État de l'art

modèles de protocoles (ex. applied $\pi$-calculus)

Problème: $\forall A_{\text{Bowser}},\ P|A_{\text{Bowser}} \approx Q|A_{\text{Bowser}}$

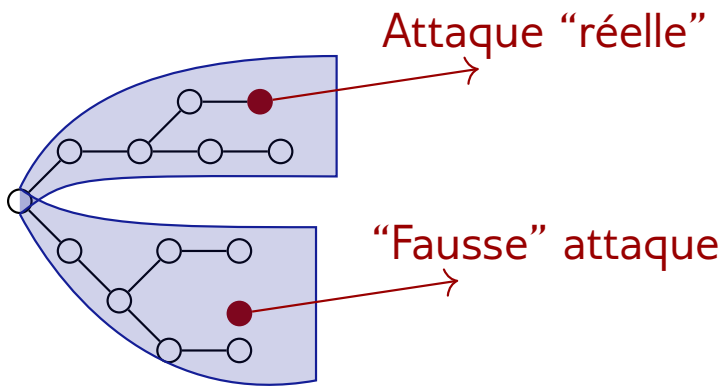
équivalence observationnelle

## Décision pour $< \infty$ sessions



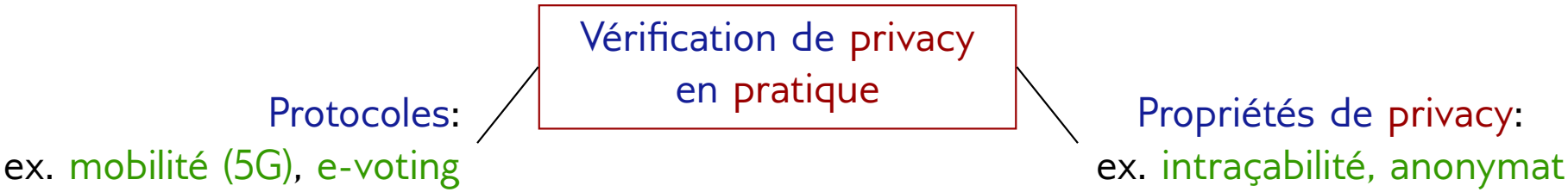

- borner le nombre de sessions
- sémantique symbolique
- exploration exhaustive des exécutions symboliques
- Outils: **Explosion # états**

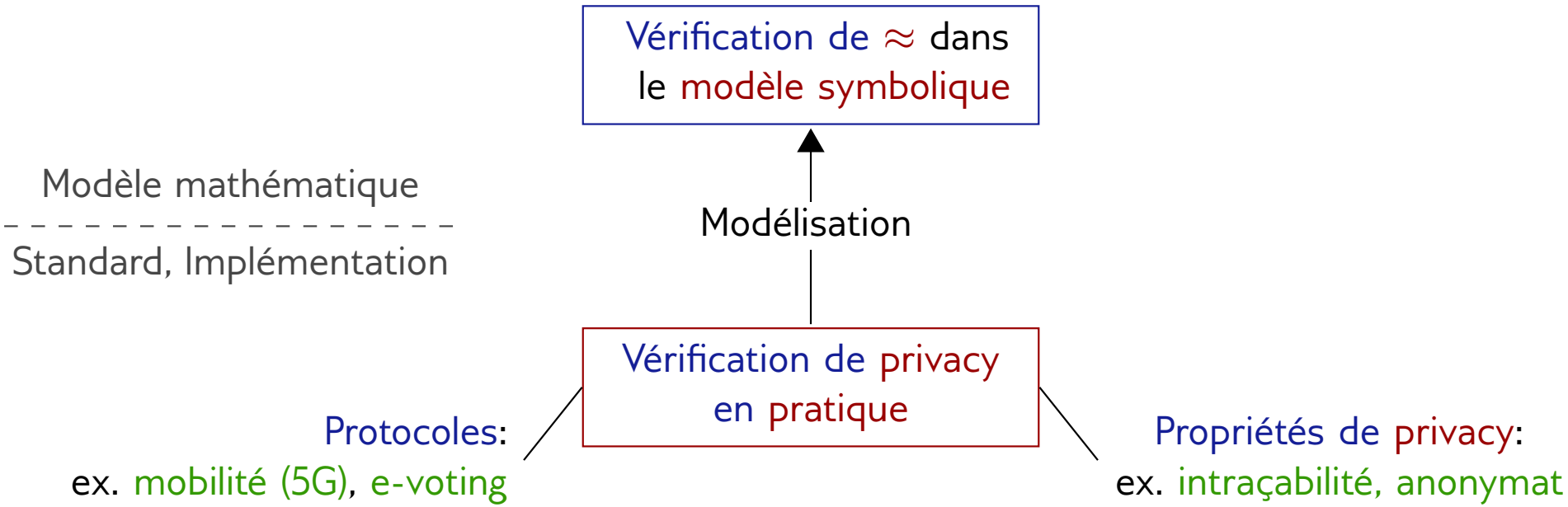
## Semi-décision pour $\infty$ sessions



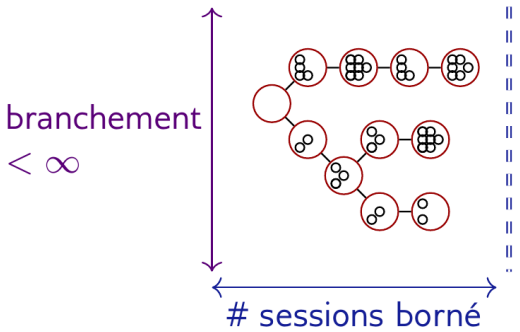

- sur-approximations de l'Bowser & la sémantique
- forme forte d'$\approx$ (*i.e.* diff-equivalence)
- Outils: **Faible précision**

Standard, Implémentation

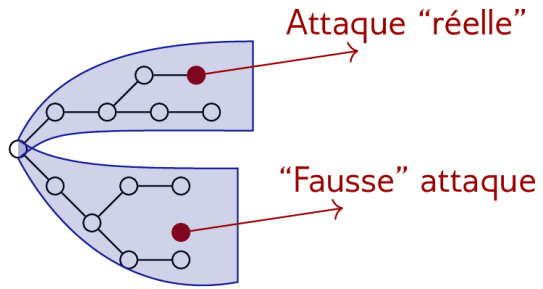



Vérification de ≈ dans
le modèle symbolique
Modèle mathématique
Standard, Implémentation
Modélisation
Vérification de privacy
en pratique
Protocoles:
ex. mobilité (5G), e-voting
Propriétés de privacy:
ex. intraçabilité, anonymat

## Décision pour $< \infty$ sessions




## Semi-décision pour $\infty$ sessions




Explosion # états

Précision

Vérification de $\approx$ dans le modèle symbolique

Modèle mathématique

Standard, Implémentation

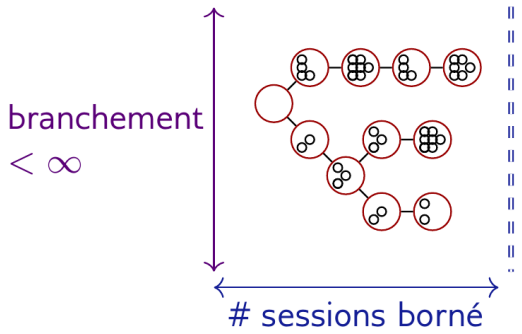
Modélisation

Vérification de privacy en pratique

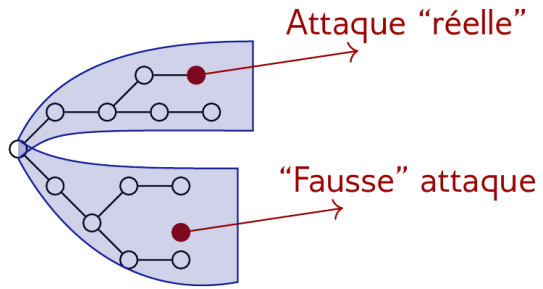
Protocoles:
ex. mobilité (5G), e-voting

Propriétés de privacy:
ex. intraçabilité, anonymat

## Décision pour $< \infty$ sessions




## Semi-décision pour $\infty$ sessions




JLAMP

CONCUR'15,
LMCS, POST'14

S&P'16

**Explosion # états**

**Précision**

Vérification de $\approx$ dans
le modèle symbolique

Modèle mathématique

Standard, Implémentation

Modélisation

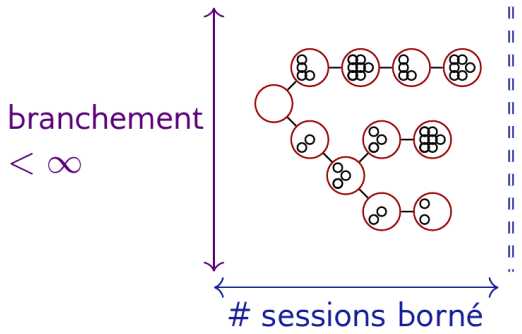
Vérification de privacy
en pratique

Protocoles:
ex. mobilité (5G), e-voting

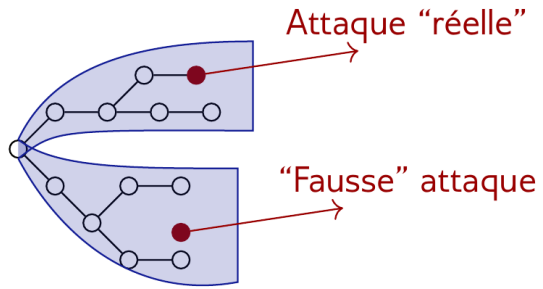
B-H USA'17, MoST'17

Propriétés de privacy:
ex. intraçabilité, anonymat

Décision pour $< \infty$ sessions




Semi-décision pour $\infty$ sessions




JLAMP

CONCUR'15, LMCS, POST'14

**Partial Order Reduction**

S&P'16

Explosion # états

Précision

Vérification de $\approx$ dans le modèle symbolique

Modèle mathématique

Standard, Implémentation

Modélisation

Vérification de privacy en pratique

Protocoles:
ex. mobilité (5G), e-voting

B-H USA'17, MoST'17

Propriétés de privacy:
ex. intraçabilité, anonymat

# Partial Order Reduction

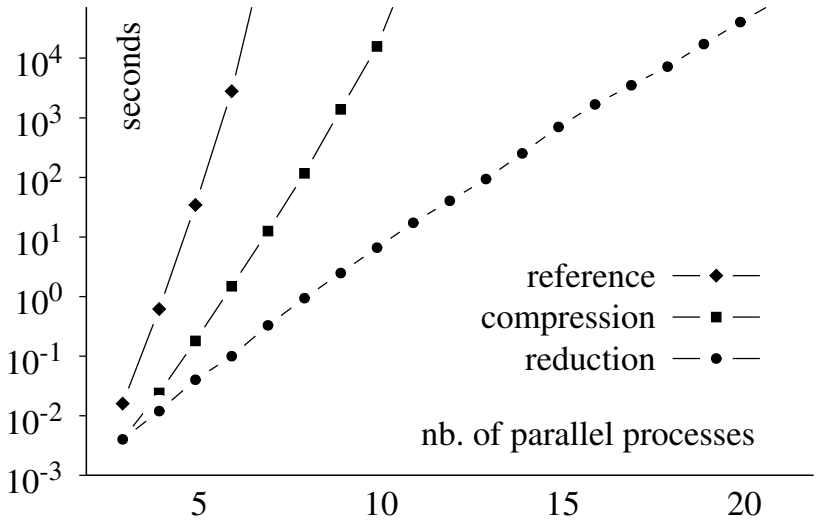
Théorie. Pour une classe de protocoles (action-deterministic):

- Techniques de Partial Order Reduction (model-checking)
- s'inspirant du Focusing (théorie de la preuve)

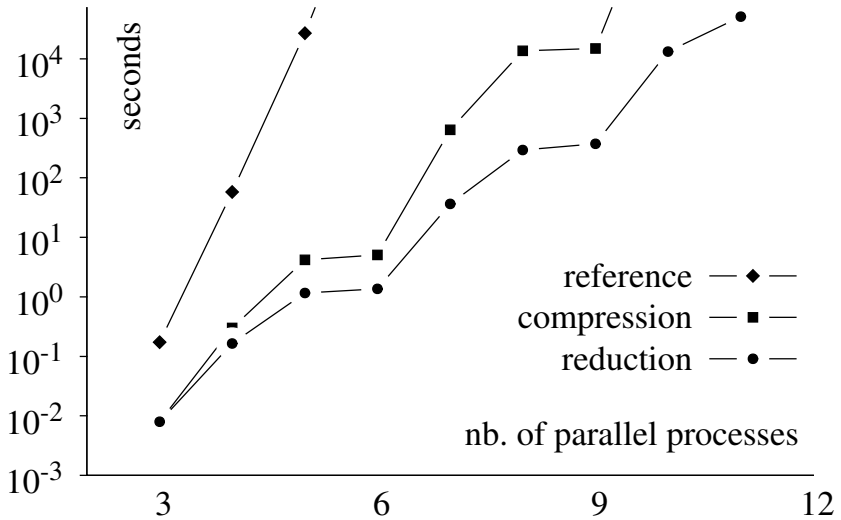
$\rightsquigarrow$ Sémantique réduite $\rightsquigarrow$ explore $\ominus$ exécutions redondantes

Pratique.

- Intégration dans Apte, DeepSec, Akiss, Spec
- Speedup jusqu'à $10^5$

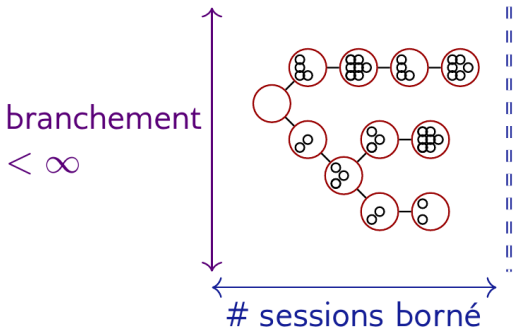



Exemple jouet

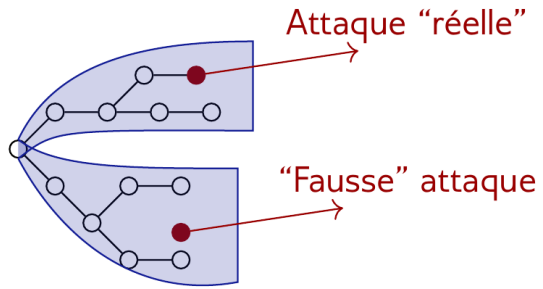



Wide Mouthed Frog

## Décision pour $< \infty$ sessions




## Semi-décision pour $\infty$ sessions




JLAMP

CONCUR'15,
LMCS, POST'14

**Conditions suffisantes pour la privacy** S&P'16

Explosion # états

Précision

Vérification de $\approx$ dans le modèle symbolique

Modèle mathématique

Standard, Implémentation

Modélisation

Vérification de privacy en pratique

Protocoles:
ex. mobilité (5G), e-voting

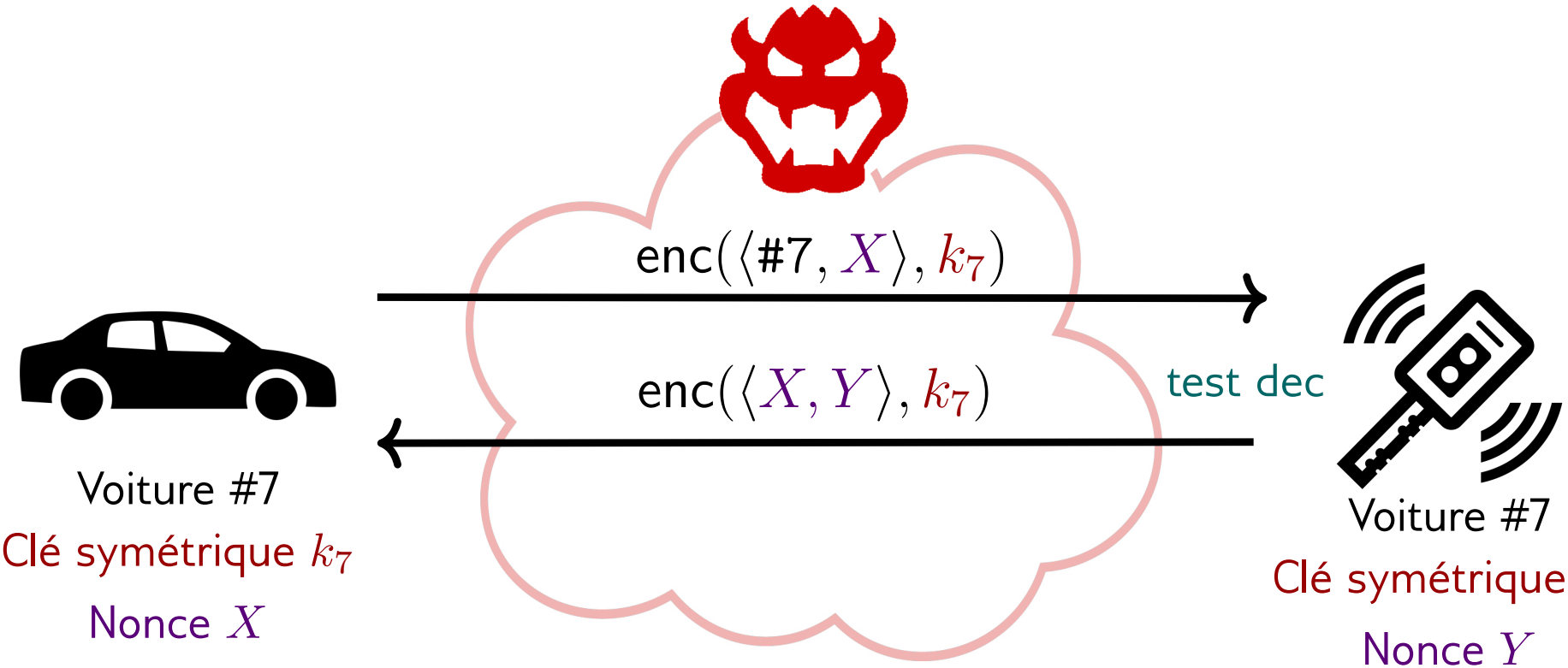
B-H USA'17, MoST'17

Propriétés de privacy:
ex. intraçabilité, anonymat

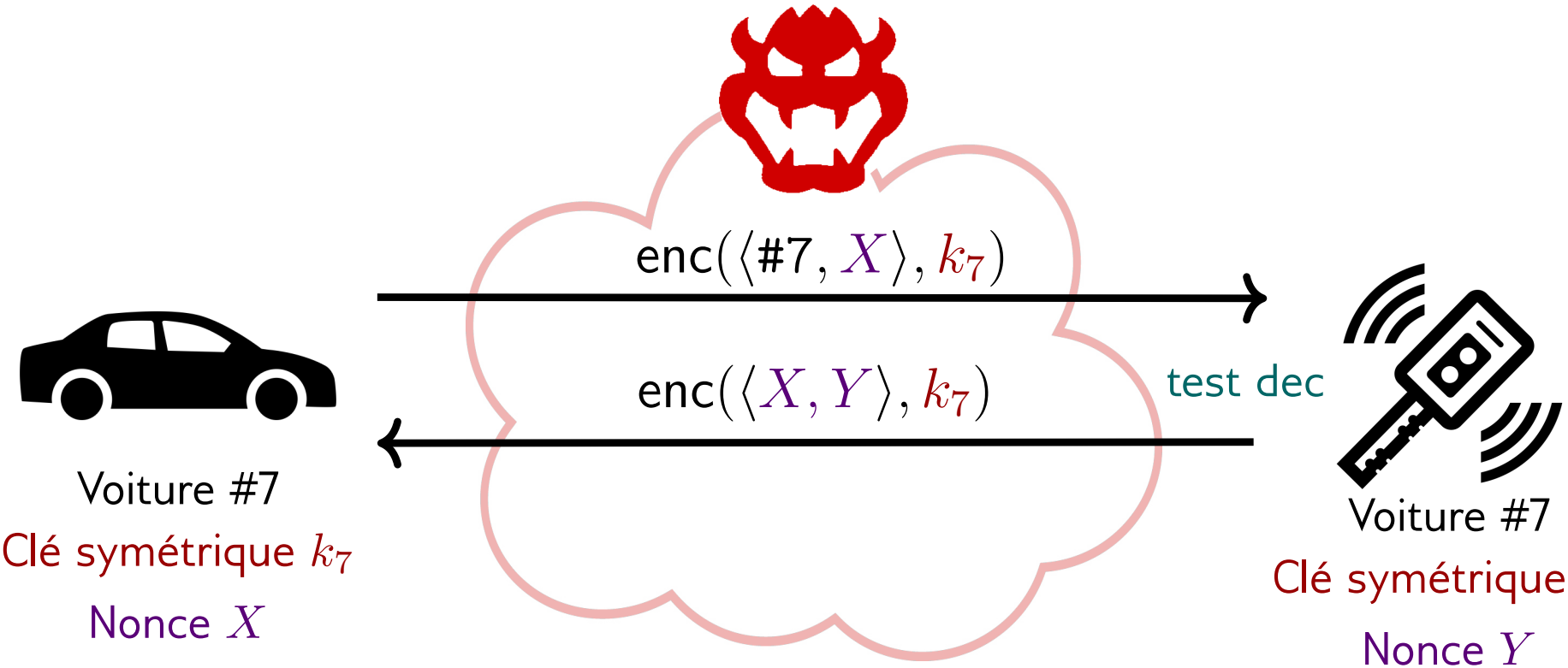
# Conditions suffisantes pour la privacy

[**H.**, Baelde, Delaune: Security & Privacy'16]

# Exemple


enc(⟨#7, X⟩, k7)
enc(⟨X, Y⟩, k7)
test dec
Voiture #7
Clé symétrique k7
Nonce X
Voiture #7
Clé symétrique k7
Nonce Y

# Exemple




Authentification: ✓

Intraçabilité: ?

# Intraçabilité

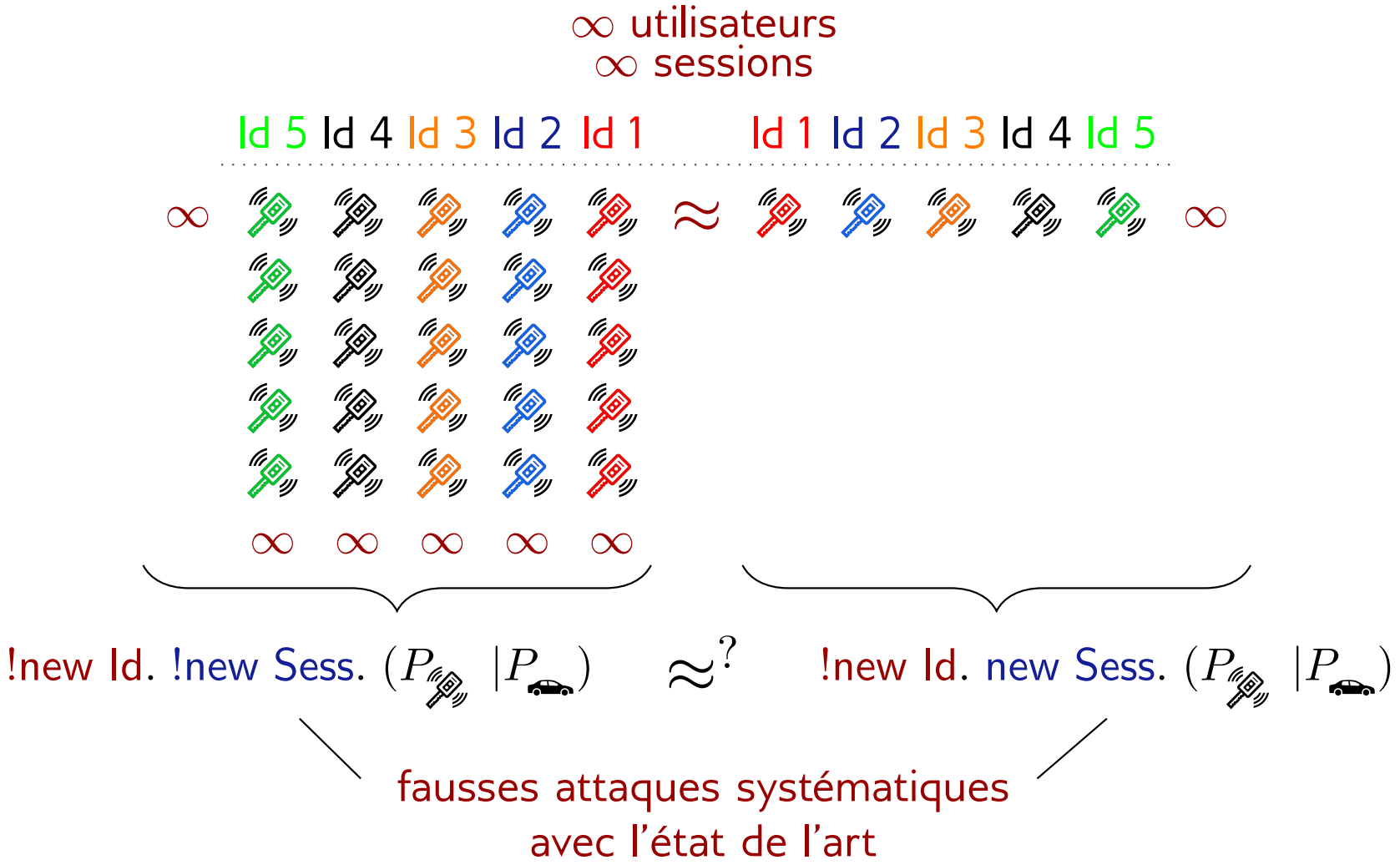
[ISO/IEC 15408] *Assure que l'utilisateur peut utiliser le système plusieurs fois sans que les autres puissent relier ces utilisations.*

1 utilisateur
2 sessions

Id 1 Id 1 Id 2

# Intraçabilité

[ISO/IEC 15408] *Assure que l'utilisateur peut utiliser le système plusieurs fois sans que les autres puissent relier ces utilisations.*



# Contributions

## Approche novatrice

- conditions suffisantes pour la privacy, dont propriété d'accessibilité
- chaque condition capture une classe d'attaques (modularité)

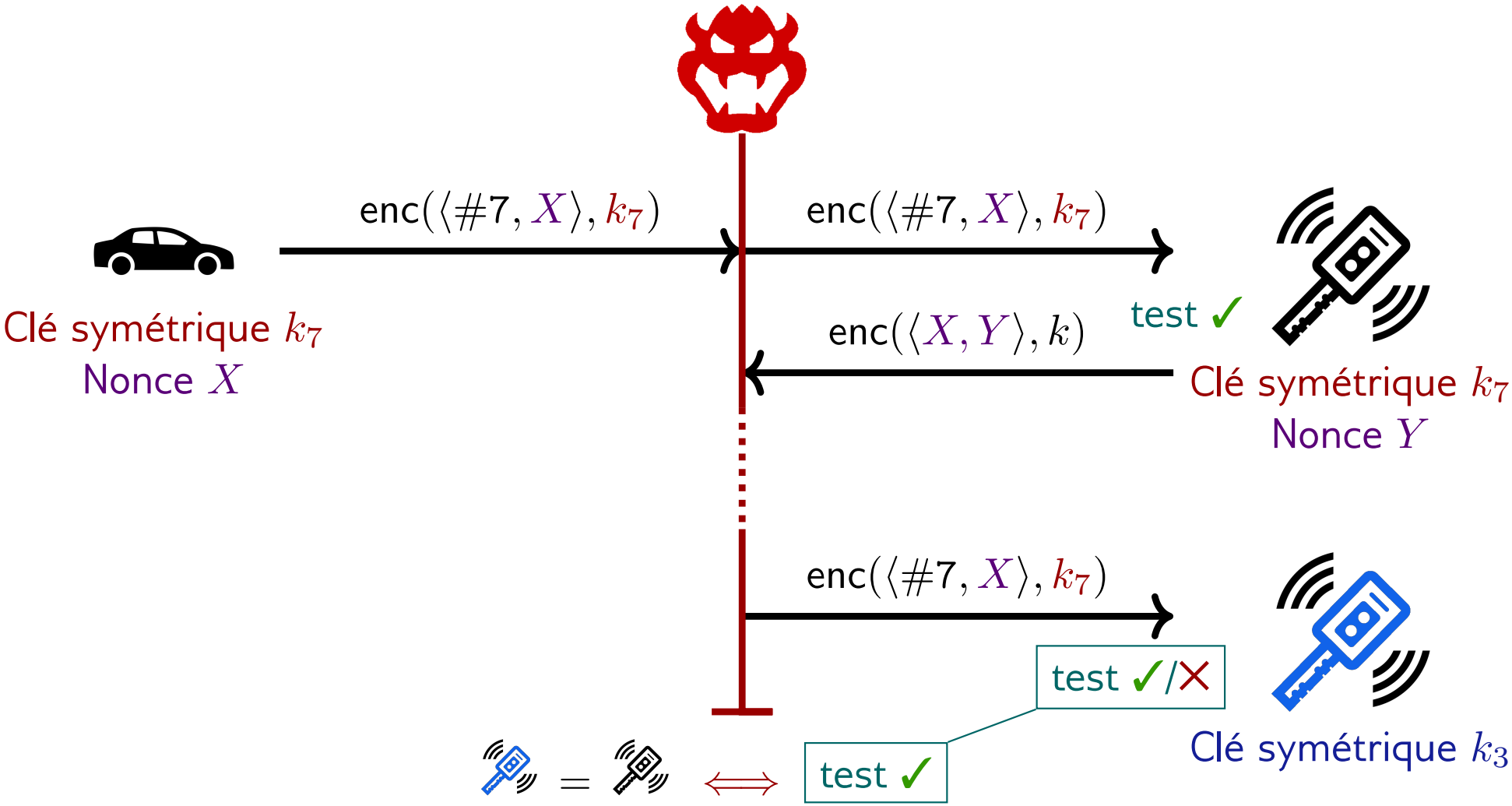
## Théorie

- 2 conditions impliquant intraçabilité et anonymat
- large classe de protocoles 2-parties
- chaque condition est fondamentalement plus simple (modularité)

## Pratique

- les 2 conditions sont vérifiables automatiquement avec précision
- développement de l'outil UKano: vérification "push-button"
- nouvelles preuves & attaques sur des protocoles industriels *e.g.* e-passport

# Un exemple dans la 1ère classe d'attaques




∃ comportement de  t.q. une conditionnelle révèle la présence d'agents

# 1ère Condition

## 1ère classe d'attaques

$\exists$ comportement de  t.q. une conditionnelle révèle la présence d'agents

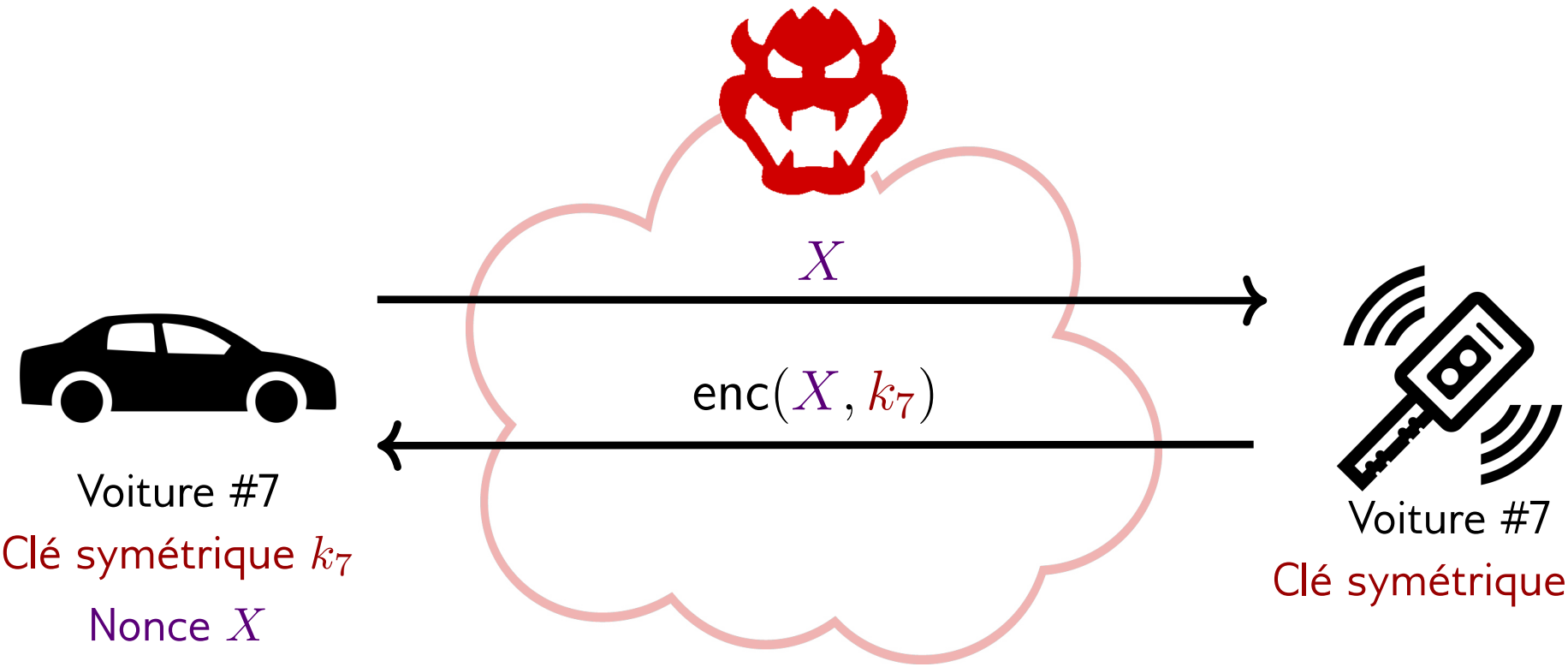
Idées pour concevoir une condition capturant ces attaques:

- Par convention:  n'interfère pas $\Rightarrow$ test ✓
- Problématique quand:  a interféré $\Rightarrow$ test ✓/✗ selon l'agent
- Condition 1: test ✓ $\iff$  n'a pas interféré pour l'agent évaluant ce test

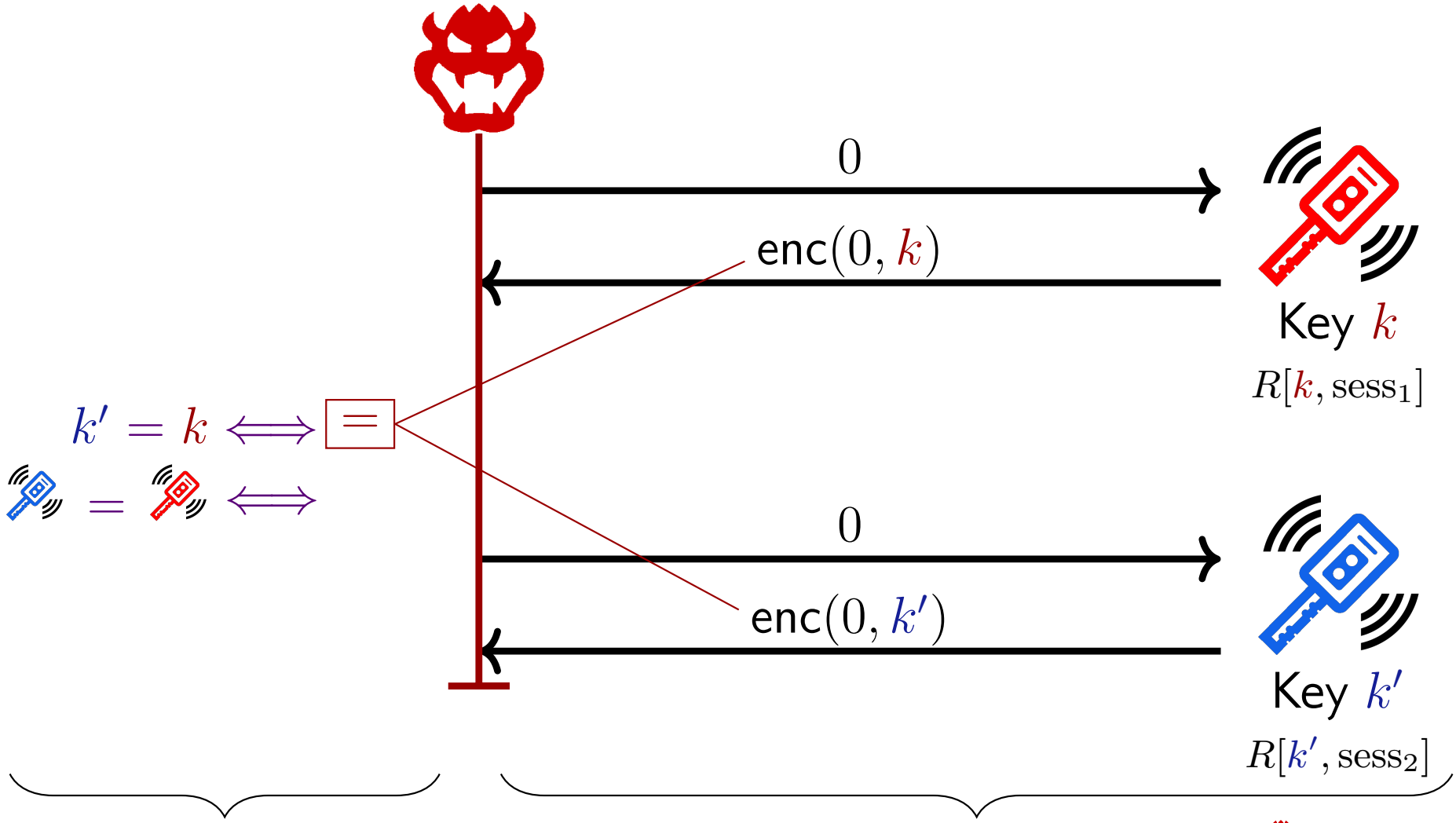
## Condition 1

Fondamentalement plus simple: propriété d'accessibilité

# Un fix ?


$X$
enc$(X, k_7)$
Voiture #7
Clé symétrique $k_7$
Nonce $X$
Voiture #7
Clé symétrique $k_7$

# Un exemple dans la 2nde classe d'attaques




Pour un comportement de l'...

... ∃ relation entre messages qui révèle la présence d'agents.

# 2nde Condition

## 2nde classe d'attaques

$\exists$ comportement de  t.q. une relation entre messages révèle la présence d'agents

Idées pour concevoir une condition capturant ces attaques:

- capturer relation entre messages non uniformes en les identités
- Condition 2: $\forall$ exécution produisant des messages $M$,

$$M \quad \sim \quad \underbrace{\mathsf{Ideal}(M)}_{\text{uniforme par définition}}$$

## Condition 2

Fondamentalement plus simple: équivalence statique sur les messages

# Le résultat

**Théorème**

Tout protocole dans la classe qui vérifie les deux conditions assure intraçabilité et anonymat.

Résumé de l'approche:

- modularité:

  chaque condition capture 1 classe d'attaques, 1 aspect de la propritété

- simplification graduelle:

  condition 2 peut se concentrer sur les exécutions satisfaisants condition 1

# Impact pratique

Outil UKano: modèle → encode les deux conditions → ProVerif → ✓/🐲/?

| Protocoles RFID | C2 | C1 | Intra. |
|---|---|---|---|
| Feldhofer | ✓ | ✓ | **prouvé** |
| Hash-Lock | ✓ | ✓ | **prouvé** |
| LAK (stateless) | – | × | 🐲 |
| Fixed LAK | ✓ | ✓ | **prouvé** |

| [*] | C2 | C1 | Intra. |
|---|---|---|---|
| DAA sign | ✓ | ✓ | **prouvé** |
| DAA join | ✓ | ✓ | **prouvé** |
| abcdh (irma) | ✓ | ✓ | **prouvé** |

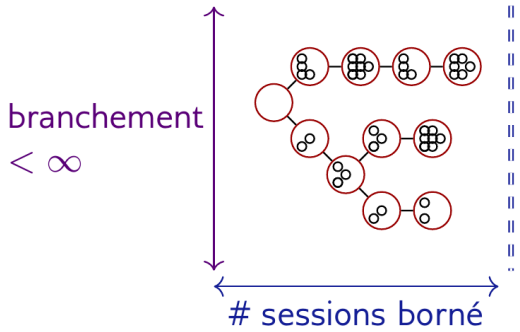
| E-passeport | C2 | C1 | Intra. |
|---|---|---|---|
| BAC | ✓ | ✓ | **prouvé** |
| BAC/PA/AA | ✓ | ✓ | **prouvé** |
| PACE (dec faillible) | – | × | 🐲 |
| PACE (test manquant) | – | × | 🐲 |
| PACE | – | × | 🐲 |
| PACE avec tags | ✓ | ✓ | **prouvé** |

- Nouvelles preuves et détection de nouvelles attaques grâce à UKano
- Impossible auparavant: fausses attaques systématiques sauf pour [*]
- Les conditions sont assez précises en pratique

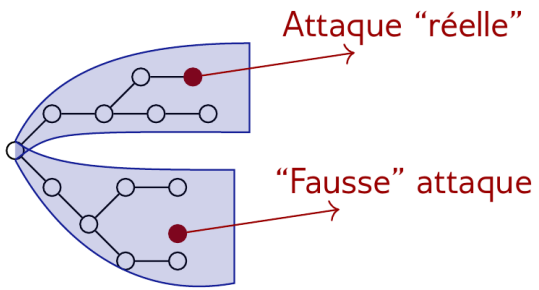
# Conclusion

# Résumé

## Décision pour $< \infty$ sessions




## Semi-décision pour $\infty$ sessions



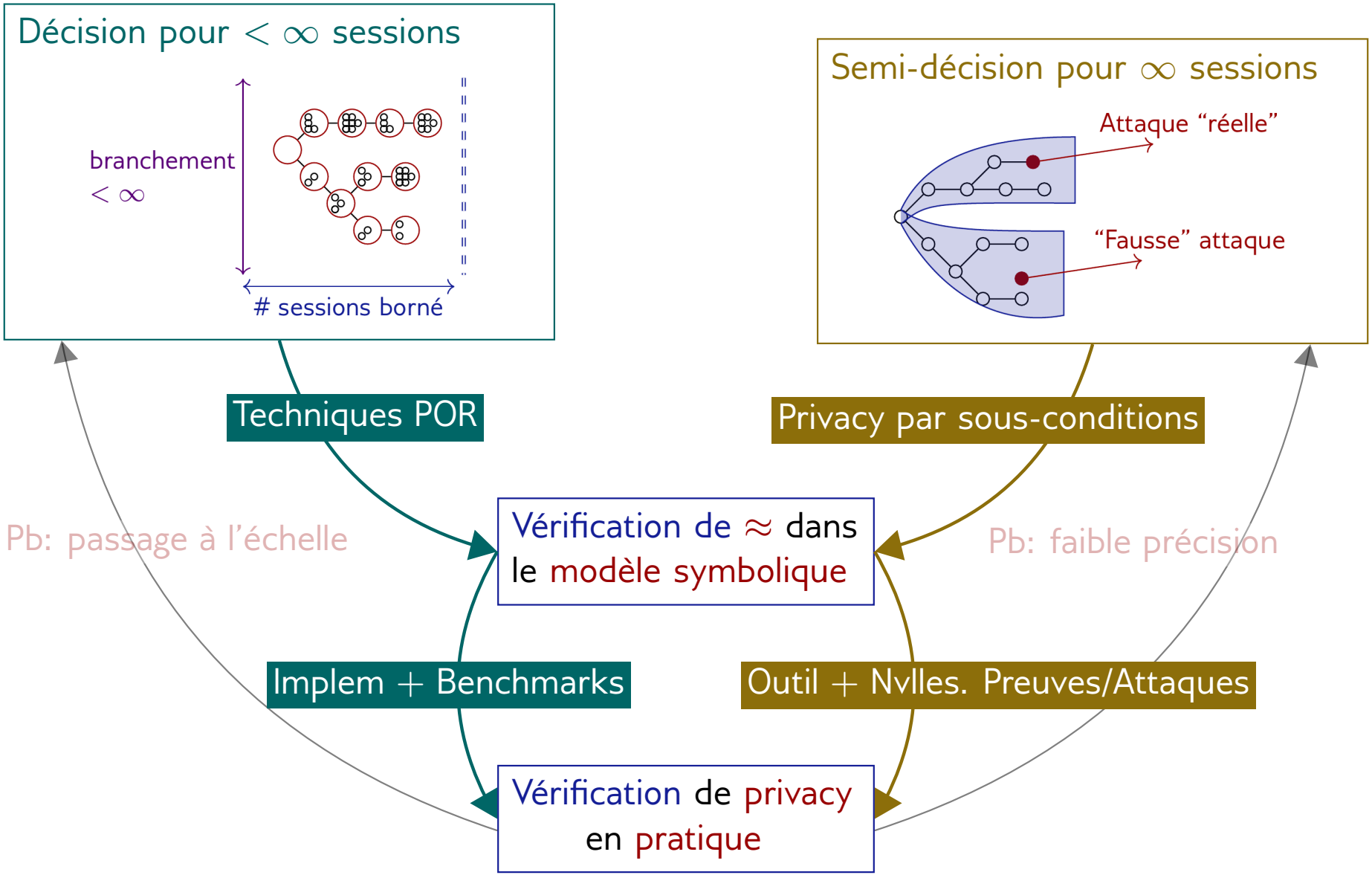

Pb: passage à l’échelle

Vérification de $\approx$ dans le modèle symbolique

Pb: faible précision

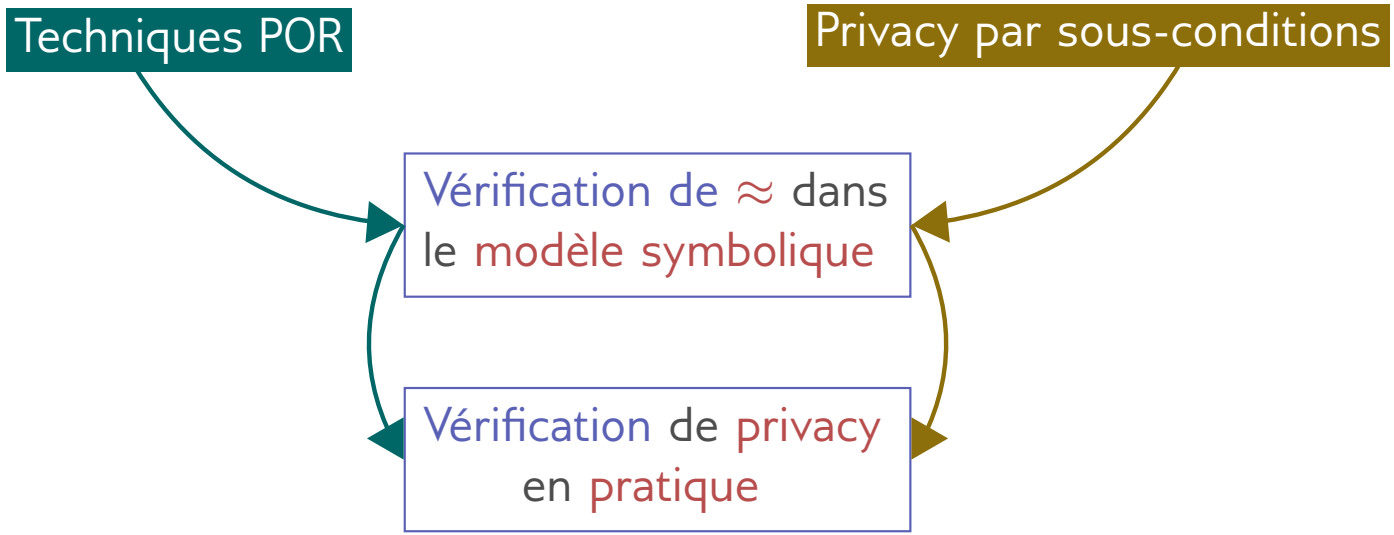
Vérification de privacy en pratique

# Résumé


Décision pour $< \infty$ sessions
branchement
$< \infty$
# sessions borné
Semi-décision pour $\infty$ sessions
Attaque "réelle"
"Fausse" attaque
Techniques POR
Privacy par sous-conditions
Pb: passage à l'échelle
Vérification de $\approx$ dans le modèle symbolique
Pb: faible précision
Implem + Benchmarks
Outil + Nvlles. Preuves/Attaques
Vérification de privacy en pratique

# Future Work

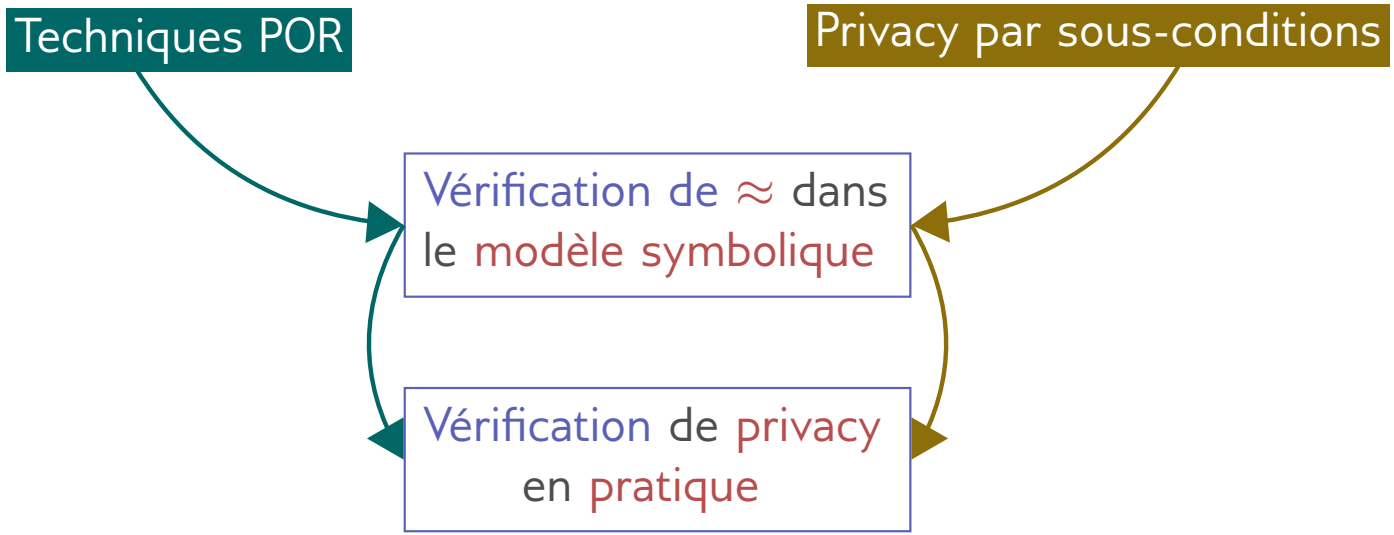
- Éliminer l'hypothèse d'action-déterminisme
- POR pour la recherche en arrière



# Future Work

- Éliminer l'hypothèse d'action-déterminisme
- POR pour la recherche en arrière

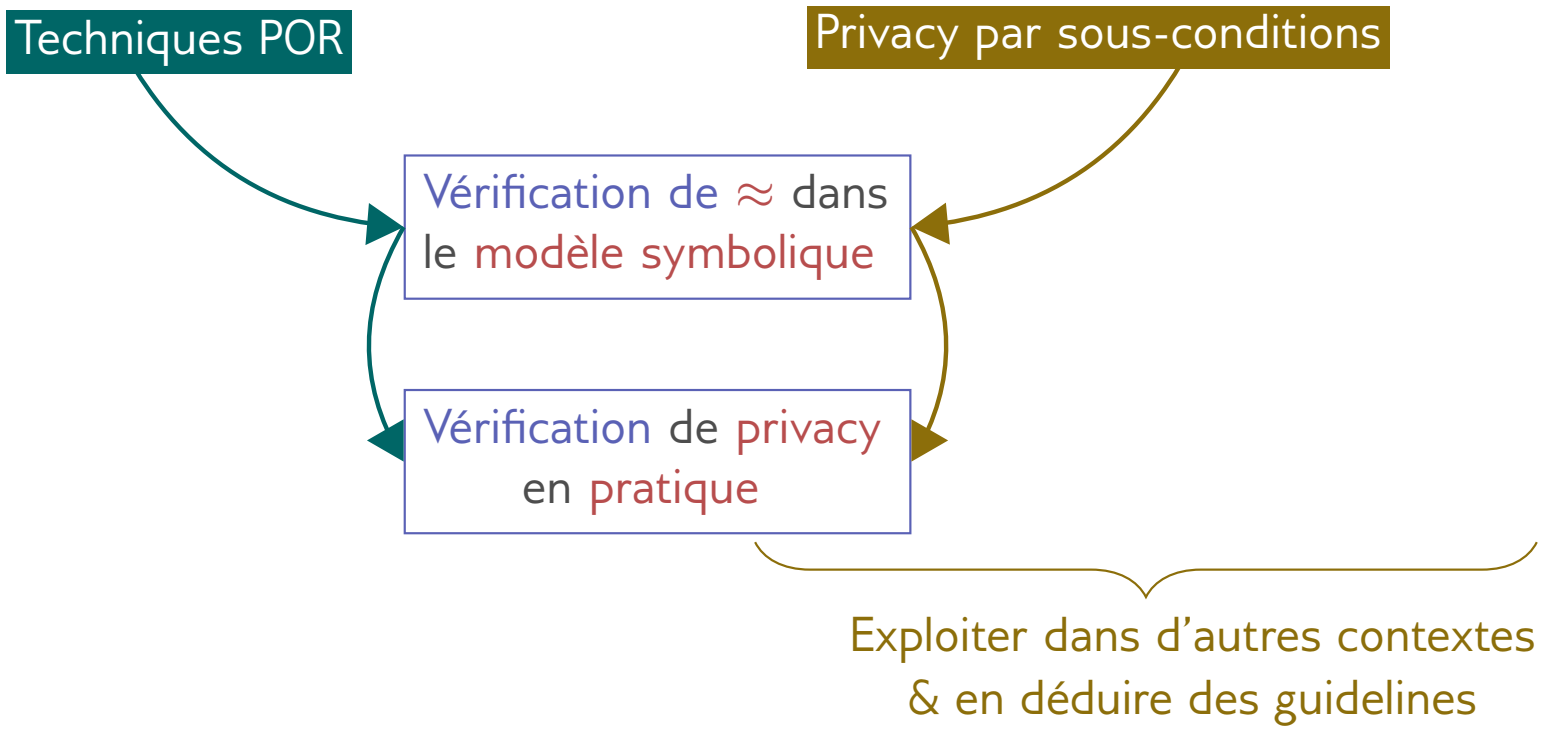
- Étendre la classe: $+$états & $>2$ parties
- Vérification de Cond2 via reachability: Untrac. & Ano. $\mapsto$ reachability pure



# Future Work

- Éliminer l'hypothèse d'action-déterminisme
- POR pour la recherche en arrière

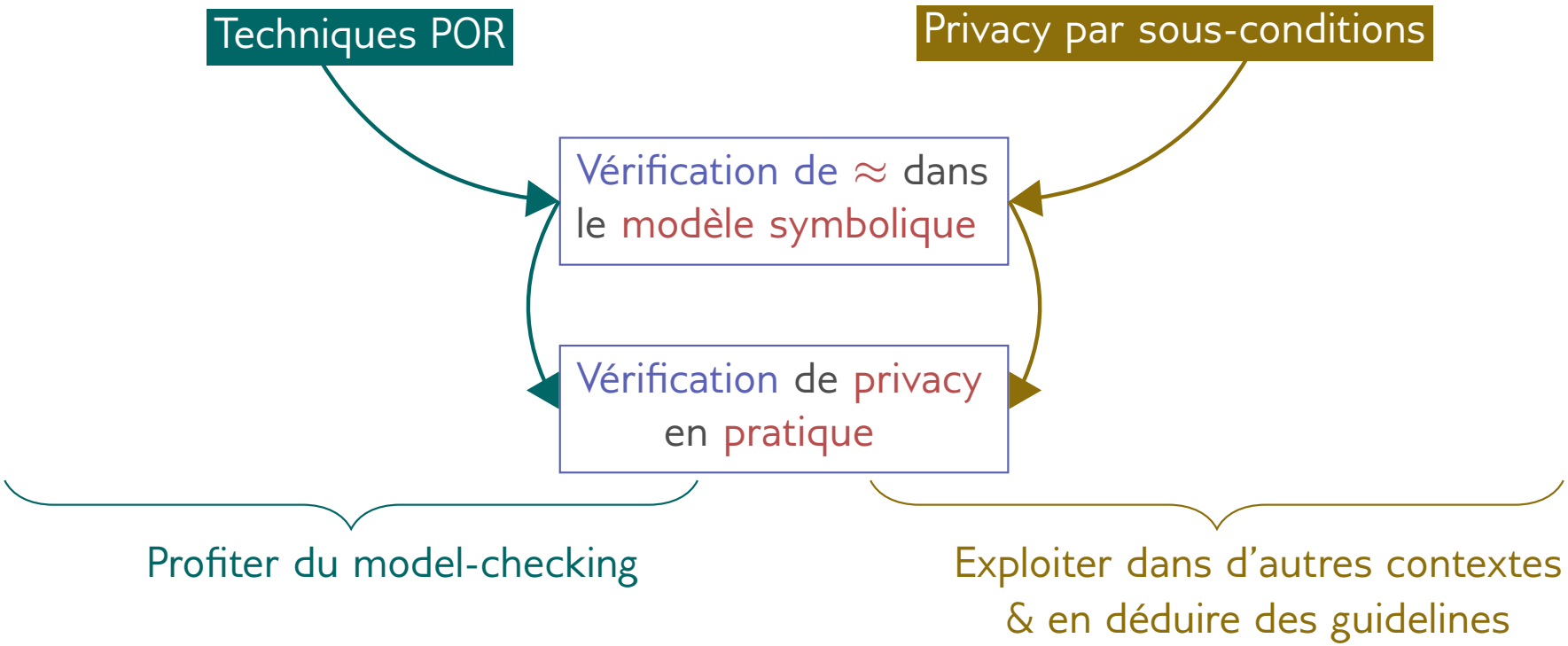
- Étendre la classe: $+$états & $>2$ parties
- Vérification de Cond2 via reachability: Untrac. & Ano. $\mapsto$ reachability pure



# Future Work

- Éliminer l'hypothèse d'action-déterminisme
- POR pour la recherche en arrière

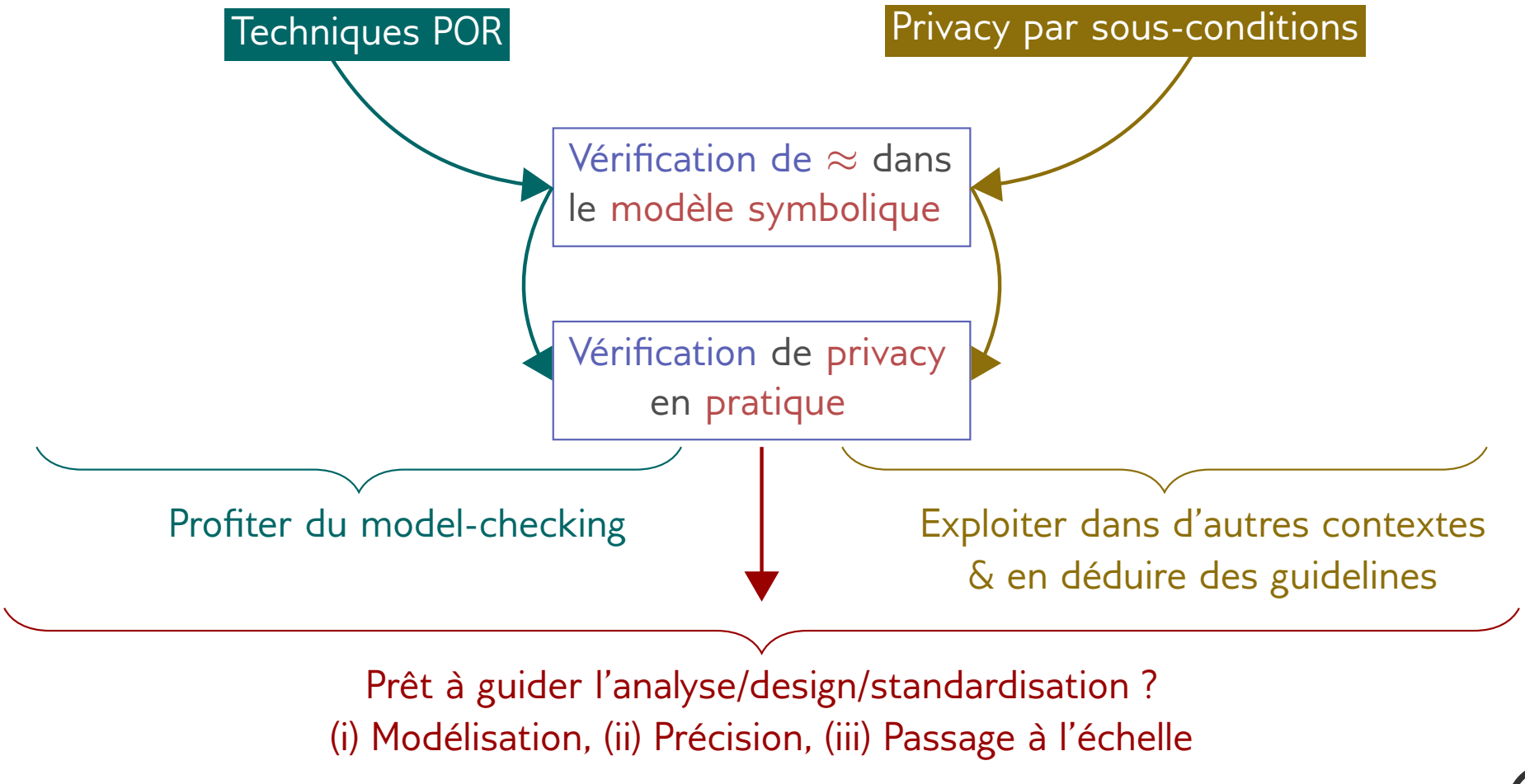
- Étendre la classe: $+$états & $>2$ parties
- Vérification de Cond2 via reachability: Untrac. & Ano. $\mapsto$ reachability pure



# Future Work

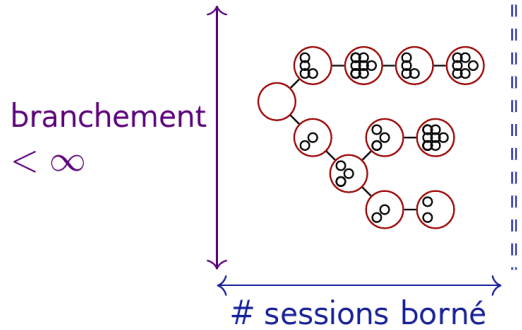
- Éliminer l'hypothèse d'action-déterminisme
- POR pour la recherche en arrière

- Étendre la classe: $+$états & $>2$ parties
- Vérification de Cond2 via reachability: Untrac. & Ano. $\mapsto$ reachability pure

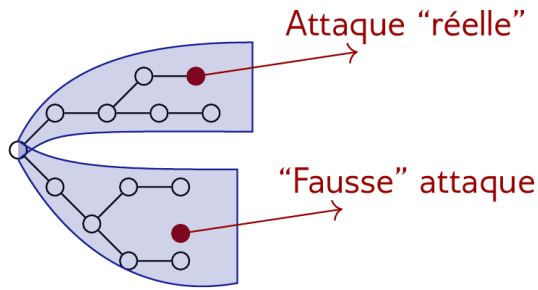


# Backup

Décision pour $< \infty$ sessions




Semi-décision pour $\infty$ sessions




3: Profiter du Model-Checking

2: Approche Hybride

Vérification de $\approx$ dans le modèle symbolique

Modèle mathématique

Standard, Implémentation

1: Compréhension Formelle de Privacy

Vérification de privacy en pratique

Protocoles:
ex. mobilité (5G), e-voting

Propriétés de privacy:
ex. intraçabilité, anonymat

# 1er Axe : Compréhension formelle de la privacy

Besoin de privacy — Modélisation → Déf. formelle dans le modèle symbolique

Exigence, *e.g.* ISO, loi

---

"Pas traçable"

ISO 15048

3GPP TS 33.849

Modélisations existantes →

$$!\mathsf{Id}.\ !\mathsf{Sess}.(P_{\text{📡}} | P_{\text{🚗}}) \approx !\mathsf{Id}.\mathsf{Sess}.(P_{\text{📡}} | P_{\text{🚗}})$$

$$(!\mathsf{Id}.\ !\mathsf{Sess}.P_{\text{📡}}) | !P_{\text{🚗}} \approx (!\mathsf{Id}.\mathsf{Sess}.P_{\text{📡}}) | !P_{\text{🚗}}$$

$$!\mathsf{Id}.\ !\mathsf{Sess}.(P_{\text{📡}} | P_{\text{🚗}}) \approx_m !\mathsf{Id}.\mathsf{Sess}.(P_{\text{📡}} | P_{\text{🚗}})$$

$$\dots$$

$\rightsquigarrow$ +15 modélisations capturant des garanties $+/-$ fortes

$\rightsquigarrow$ **comparaison?, choix?, 🐢?**

## Objectifs:

- Hiérarchisation formelle des modélisations mathématiques en général et pour des classes réalistes de protocoles (pertinence pratique des $\neq$)
- Définitions formelles des nouveaux modèles d'attaquants + vérification: compromission d'agents, post/pre-compromission, attaquant quantique.

# 2ème Axe : Approche hybride pour la privacy

- Modularité: 1 condition capture 1 classe d'attaques, 1 aspect de la propritété
- Simplification graduelle: $\text{condition}_n$ peut supposer $\text{condition}_{j<n}$
- Avantages: $+$ précisions & efficacité, modulaire, explicatif

**Objectifs:**

- Utiliser ce nouvel outil pour résoudre les nombreux problèmes de l'état de l'art:
  - E-voting: avec coercion, comptage, revote, etc. (état de l'art très limité)
  - Protocoles d'auth.: nombreuses limitations, ex. 5G ($+2$ parties, stateful)
- Unifier ces idées pour proposer un outil de vérification générique pour la privacy

Résultats préliminaires: 2 instantiations spécifiques

- Intraçabilité/anonymat: 2-parties & stateless
- Secret du vote: classe restrictive de protocoles e-voting

# 3ème Axe : Profiter des avancées en Model-Checking

Exemple: Anonymat pour *Private Authentication*: (avec Apte)
1 session $\mapsto$ 1 seconde, 2 sessions $\mapsto$ 1 heure, 3 sessions $\mapsto$ **>2 jours**.

Model-Checking:
- POR statique/dynamique
- réduction de symétries, etc.

$\rightsquigarrow$

Vérification de privacy:
- $\approx$ + attaquant
- sémantique symbolique

Objectifs:

Importer les avancées en model-checking à la sécurité:
- POR dynamique
- POR statique pour recherche en arrière
- CounterExample-Guided Abstraction Refinement

- Idéalement via un transfert direct sur un encodage de $\approx$

Résultats préliminaires: Partial Order Reduction extrêmement efficace (speedup $10^5$) mais *ad-hoc* et pour une classe restrictive de protocoles (CONCUR'15, LMCS, POST'14)