Vérification Formelle d'un Protocole de Vote

Cyrille Wiedling

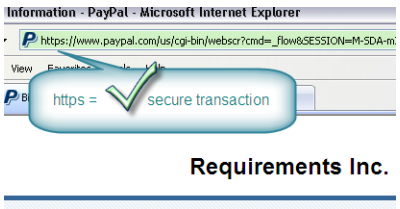
Université de Strasbourg

Soutenance de stage, 1er Septembre 2011

Stage sous la direction de Véronique Cortier.

Contexte

Les protocoles cryptographiques sont maintenant utilisés presque inconsciemment dans notre vie courante :



$\Rightarrow$ Leur but est de sécuriser les transmissions sur des réseaux publics ou non sûrs.

Définition

Qu'est-ce qu'un protocole cryptographique ?

- « Protocole » : Série d'étapes impliquant deux ou plusieurs participants pour accomplir une tâche.
(e.g. Calculer une clef privée commune, ...)

- « Cryptographique » : Qui met en jeu des fonctions à caractère cryptographique.
(e.g. Chiffrement, signature, hachage, ...)

Objectif : Sécurité

Les protocoles cryptographiques servent à :

- préserver la confidentialité des données
  (e.g. Codes PIN, dossiers médicaux, ...)
- assurer l'authenticité
  (Êtes-vous réellement entrain de parler avec votre banque ?)
- assurer l'anonymat de certaines transmissions
  (Pour les protocoles de E-vote, ...)
- assurer la non-répudiation
  (Nier l'envoi d'un message, ...)

Les Capacités d'un Intrus

Présence d'un Intrus qui

- peut participer au protocole.
- peut créer et envoyer des messages,
- peut lire tous les messages envoyés sur le réseau,
- peut intercepter des messages.

De nombreuses attaques sont possibles :

- Needham-Schroeder : Attaque découverte 17 ans plus tard !
- Google Apps : Brèche découverte en 2008 (Avantssar)

Les Capacités d'un Intrus

Présence d'un Intrus qui

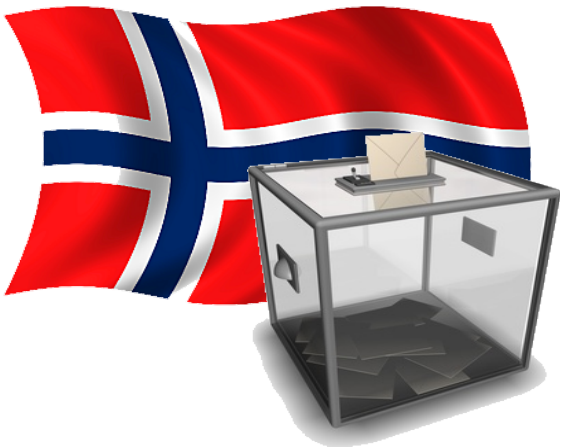
- peut participer au protocole.
- peut créer et envoyer des messages,
- peut lire tous les messages envoyés sur le réseau,
- peut intercepter des messages.

De nombreuses attaques sont possibles :

- Needham-Schroeder : Attaque découverte 17 ans plus tard !
- Google Apps : Brèche découverte en 2008 (Avantssar)

Le But du Stage

Le protocole de vote Norvégien

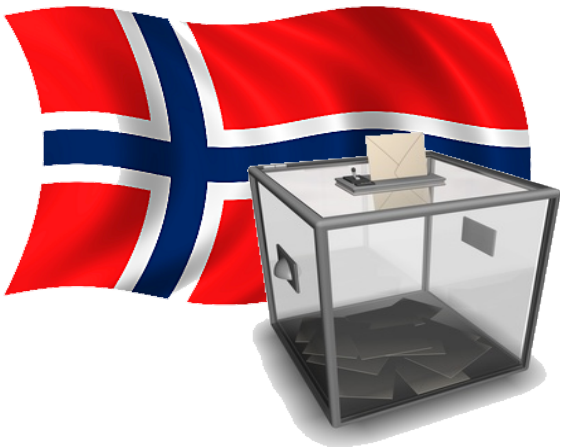


- Développé par ErgoGroup.
- Utilisation prévue dans le cadre d'élections municipales et de comtés.
- Protocole actuellement implanté et en phase de test.

Objectif du Stage : Analyser le protocole de vote Norvégien pour démontrer rigoureusement la confidentialité.

Le But du Stage

Le protocole de vote Norvégien



- Développé par ErgoGroup.
- Utilisation prévue dans le cadre d'élections municipales et de comtés.
- Protocole actuellement implanté et en phase de test.

Objectif du Stage : Analyser le protocole de vote Norvégien pour démontrer rigoureusement la confidentialité.

Comment analyser la sécurité d'un protocole ?

Comment garantir qu'un protocole vérifie la confidentialité, l'authenticité, l'anonymat... ?

Méthode

1. Proposer un modèle formel précis du protocole
2. Formaliser les propriétés de sécurité à démontrer
3. Démontrer les résultats souhaités

Modéliser les Messages

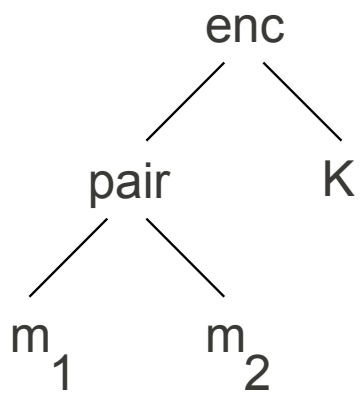
On modélise les messages par des termes.

Chiffrement : $\text{enc}(m, K)$ Concaténation : $\text{pair}(m_1, m_2)$

Exemple : Le message

$\text{enc}(\text{pair}(m_1, m_2), K)$

est représenté par l'arbre :



On modélise en conservant la structure des messages.

Les Théories équationelles

Modélisent les propriétés mathématiques des symboles utilisés.

Théorie du Chiffrement-Déchiffrement

$$\mathsf{dec}(\mathsf{enc}(x,y),y) = x \quad \pi_1(\mathsf{pair}(x,y)) = x \quad \pi_2(\mathsf{pair}(x,y)) = y$$

Théorie du OU Exclusif

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z \quad x \oplus y = y \oplus x$$
$$x \oplus x = 0 \qquad x \oplus 0 = x$$

Les Théories équationelles

Modélisent les propriétés mathématiques des symboles utilisés.

Théorie du Chiffrement-Déchiffrement

$$\mathrm{dec}(\mathrm{enc}(x,y),y) = x \quad \pi_1(\mathrm{pair}(x,y)) = x \quad \pi_2(\mathrm{pair}(x,y)) = y$$

Théorie du OU Exclusif

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z \quad x \oplus y = y \oplus x$$
$$x \oplus x = 0 \qquad x \oplus 0 = x$$

Formaliser la Confidentialité

Comment formuler correctement :

"Personne ne doit découvrir mon vote (0 ou 1)." ?

Formaliser la Confidentialité

Comment formuler correctement :

"Personne ne doit découvrir mon vote (0 ou 1)." ?

Idée : On ne doit pas découvrir la valeur de mon vote.

Formaliser la Confidentialité

Comment formuler correctement :

"Personne ne doit découvrir mon vote (0 ou 1)." ?

~~Idée : On ne doit pas découvrir la valeur de mon vote.~~

Confidentialité (S. Kremer & M. Ryan)

Un protocole vérifie la confidentialité si un intrus ne voit pas de différence lorsque les votes sont échangés.

$$\text{Voter}_1(0) \mid \text{Voter}_2(1) \sim \text{Voter}_1(1) \mid \text{Voter}_2(0)$$

Comment Démontrer ?

Il existe des outils de vérification automatique très performants :
(ProVerif, Avispa/Avantssar, Scyther, ...)

- Ils permettent de détecter des attaques,
- de démontrer la sécurité de protocoles standard

Mais les outils ne fonctionnent pas sur les protocoles de vote !
(Notamment sur le protocole de vote Norvégien)

- La modélisation des protocoles de vote est souvent complexe et sort du champ d'action assez limité des outils.
- Les propriétés d'équivalence sont peu ou pas traitées par ces outils.

Comment Démontrer ?

Il existe des outils de vérification automatique très performants :
(ProVerif, Avispa/Avantssar, Scyther, ...)

- Ils permettent de détecter des attaques,
- de démontrer la sécurité de protocoles standard

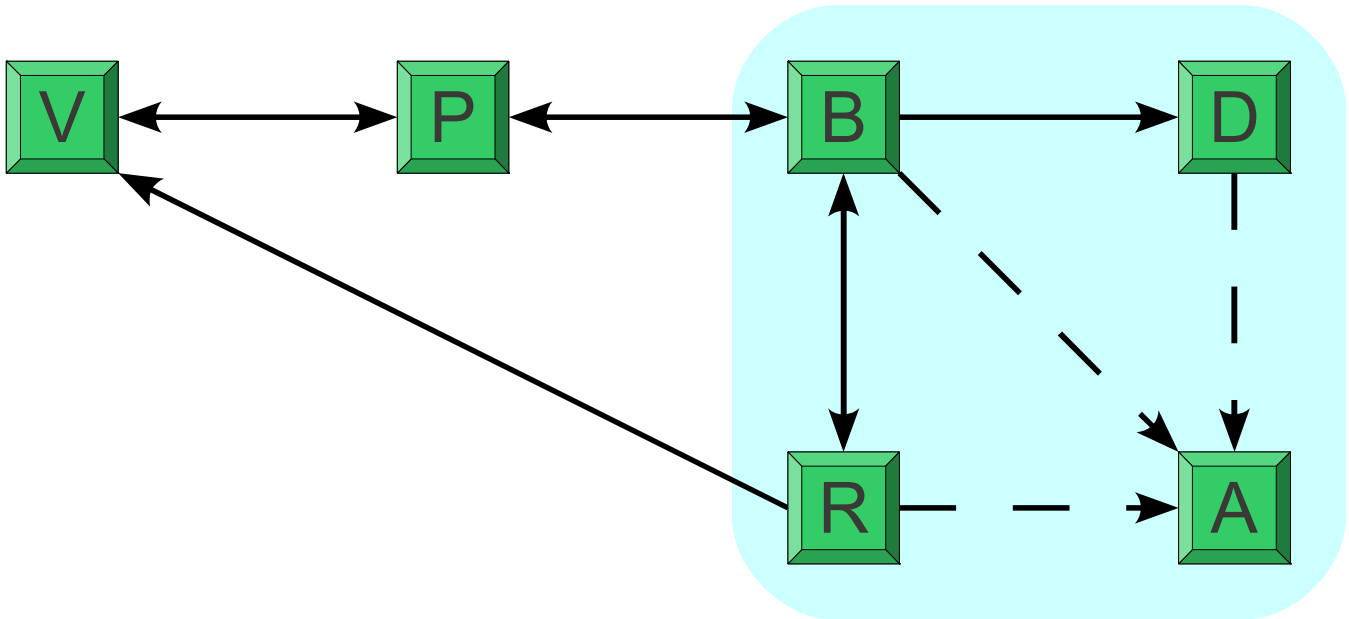
Mais les outils ne fonctionnent pas sur les protocoles de vote !
(Notamment sur le protocole de vote Norvégien)

- La modélisation des protocoles de vote est souvent complexe et sort du champ d'action assez limité des outils.
- Les propriétés d'équivalence sont peu ou pas traitées par ces outils.

Mes contributions

1. Modélisation formelle du protocole.
2. Preuve à la main de la confidentialité.
3. Application de ProVerif à une version simplifiée du protocole.

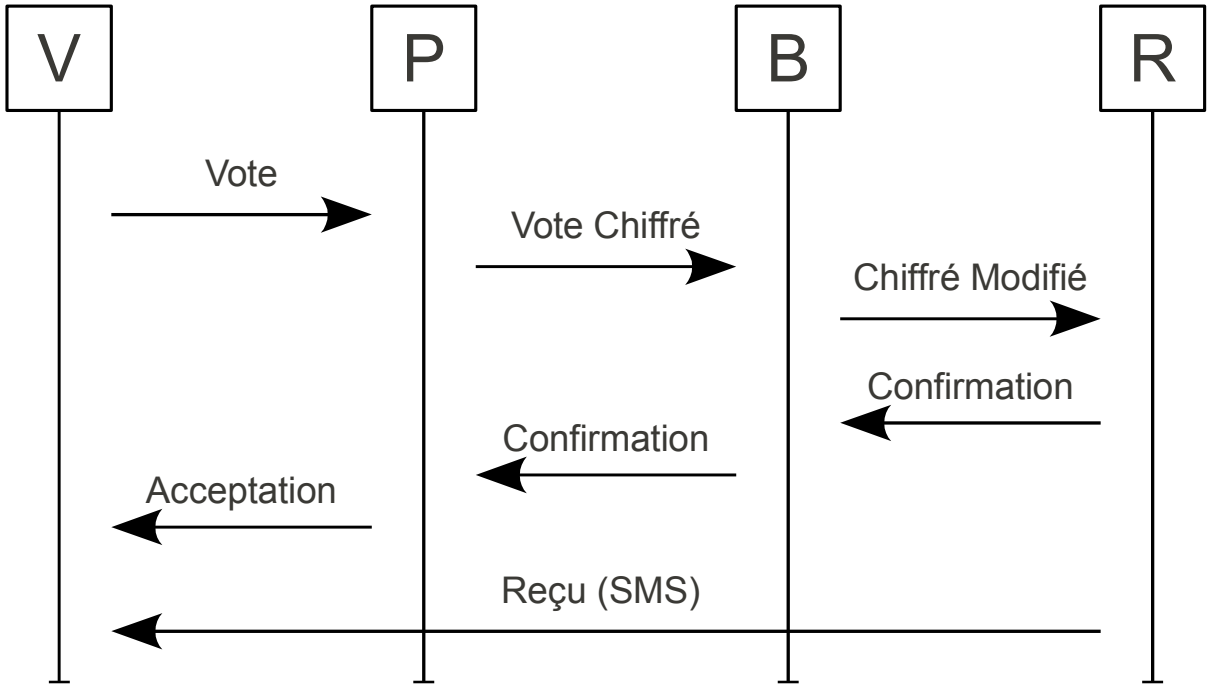
Protocole de Vote Norvégien : Les différents acteurs



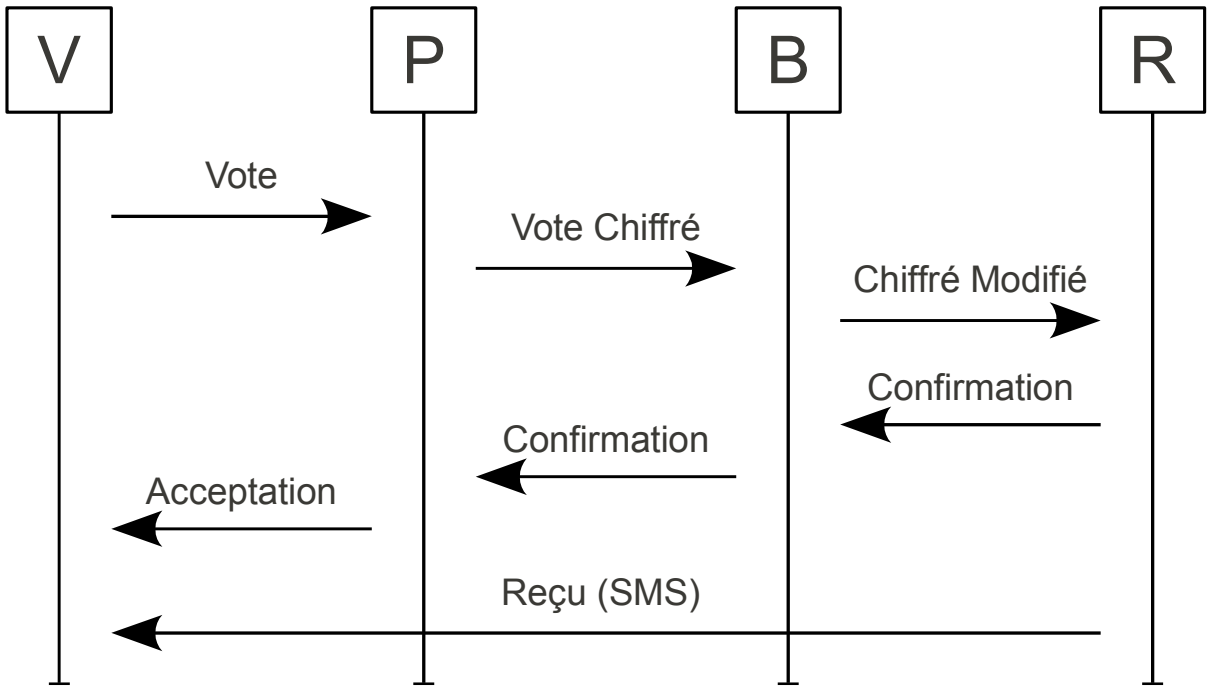
V : Votant R : Générateur de reçus B : Urne
P : Ordinateur D : Déchiffreur A : Auditeur

Protocole de Vote Norvégien : Le principe

Schéma de soumission d'un vote



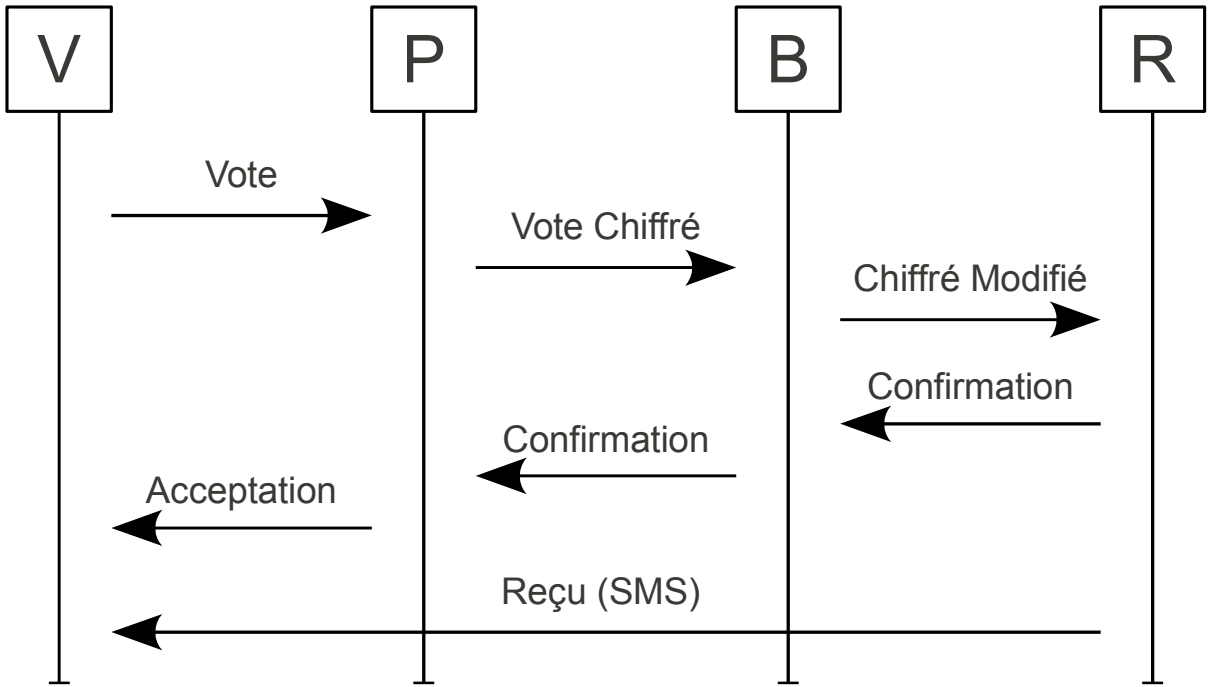
Protocole de Vote Norvégien : Le principe



Vote Chiffré :

$$(\mathrm{penc}(v, r, \mathrm{pk}(a_1)), \mathrm{pfk}_1(id, r, v, \mathrm{penc}(v, r, \mathrm{pk}(a_1))),$$
$$\mathrm{sign}(\mathrm{pair}(\mathrm{penc}(v, r, \mathrm{pk}(a_1)), \mathrm{pfk}_1(id, r, v, \mathrm{penc}(v, r, \mathrm{pk}(a_1)))), id))$$

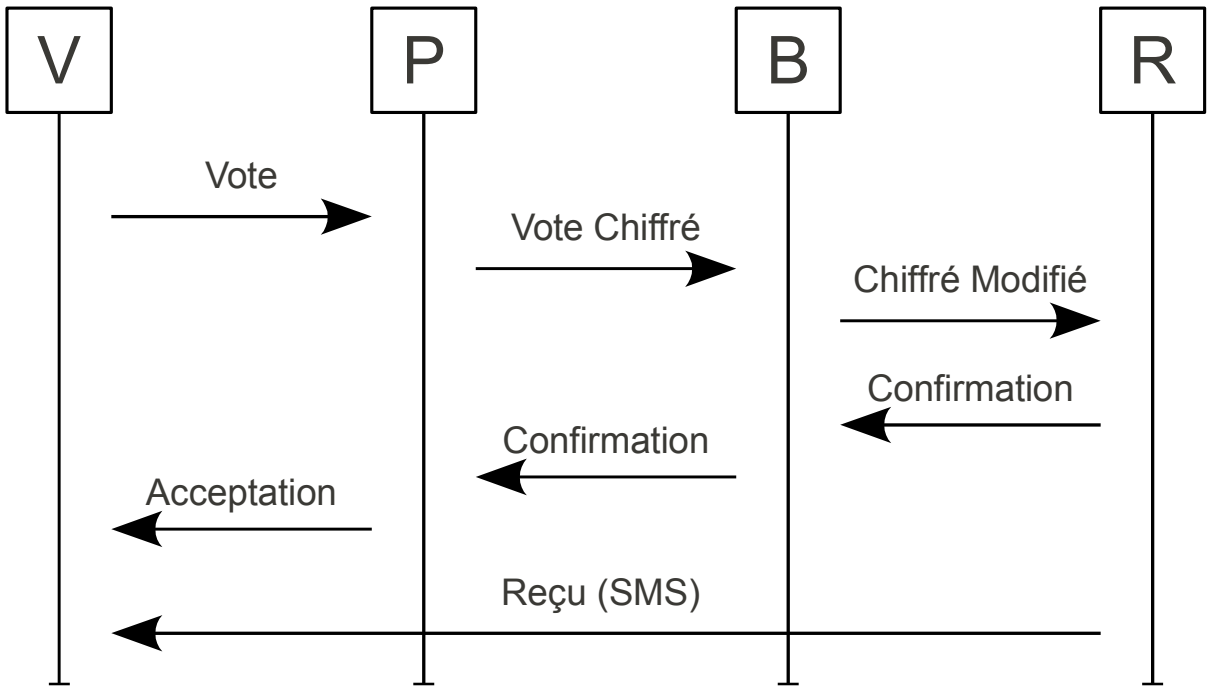
Protocole de Vote Norvégien : Le principe



Chiffré Modifié :

$$(\mathrm{blind}(\mathrm{renc}(\mathrm{penc}(v, r, \mathrm{pk}(a_1)), a_2), \mathrm{s}(id)), \mathrm{pfk}_2(\ldots), \ldots)$$

Protocole de Vote Norvégien : Le principe



Reçu :

$$\mathrm{dec}(\mathrm{blind}(\mathrm{renc}(\mathrm{penc}(v, r, \mathrm{pk}(a_1)), a_2), \mathrm{s}(id)), a_3)$$

Modélisation : les Messages

Signature

$$\Sigma = \{\mathsf{OK}, \mathsf{fst}, \mathsf{hash}, \mathsf{pk}, \mathsf{s}, \mathsf{snd}, \mathsf{vk}, \mathsf{blind}, \mathsf{dec}, +, *, \circ, \diamond, \mathsf{pair}$$
$$\mathsf{renc}, \mathsf{sign}, \mathsf{unblind}, \mathsf{checkpfk}_1, \mathsf{checkpfk}_2, \mathsf{checksign}, \mathsf{penc}, \mathsf{pfk}_1, \mathsf{pfk}_2\}$$

(1) $\mathsf{fst}(\mathsf{pair}(x, y)) = x$

(2) $\mathsf{snd}(\mathsf{pair}(x, y)) = y$

(3) $\mathsf{dec}(\mathsf{penc}(x_{plain}, x_{rand}, \mathsf{pk}(x_{sk})), x_{sk}) = x_{plain}$

(4) $\mathsf{dec}(\mathsf{blind}(\mathsf{penc}(x_p, x_r, \mathsf{pk}(x_{sk})), x_b), x_{sk}) = \mathsf{blind}(x_p, x_b)$

(5) Six autres équations ...

Modélisation : le Protocole

Exemple d'une modélisation d'un participant (Le votant) :

$$V(c_{auth}, c_{out}, c_{RV}, g_1, id, idp_R, x_{vote}) = \nu t \ .$$
$$\text{Let } e = \text{penc}(x_{vote}, t, g_1) \text{ in}$$
$$\text{Let } p = \text{pfk}_1(id, t, x_{vote}, e) \text{ in}$$
$$\text{Let } si = \text{sign}((e, p), id) \text{ in}$$
$$\overline{c}_{auth}\langle(e, p, si)\rangle \ .$$
$$c_{auth}(x) \ . \ c_{RV}(y) \ .$$
$$\text{Let } h = \text{hash}((\text{vk}(id), e, p, si)) \text{ in}$$
$$\text{If } \phi_{\text{v}}^{idp_R}(id, h, x, x_{vote}, y) \text{ Then } \overline{c}_{out}\langle\text{OK}\rangle$$
$$\text{Else } \overline{c}_{out}\langle\text{fail}\rangle$$

Premier Résultat : Confidentialité

Résultat : Le protocole de vote Norvégien sans auditeur vérifie la propriété de confidentialité.

Théorème (Maths)

On a :

$$V(id_1, 0)|V(id_2, 1)|B(\dots)|R(\dots)|D(\dots) \equiv V(id_1, 1)|V(id_2, 0)|B(\dots)|R(\dots)|D(\dots)$$

Avec $\equiv$, une relation d'équivalence telle que :

1. Bisimilarité : $P \equiv Q$ et $P \to P'$, $Q \to Q'$ alors $P' \equiv Q'$.
2. Les messages sont équivalents du point de vue de l'intrus.

Idée de la Démonstration

1. Trouver une sur-approximation de la bisimulation.

   On crée une relation de toute pièce qui convient.

2. Montrer l'équivalence entre les messages.

   L'intrus ne doit pas voir de différence entre les deux exécutions.

Idée de la Démonstration

1. Trouver une sur-approximation de la bisimulation.

   On crée une relation de toute pièce qui convient.

2. Montrer l'équivalence entre les messages.

   L'intrus ne doit pas voir de différence entre les deux exécutions.

Deuxième Résultat : Décidabilité

Décidabilité de la capacité de calcul de l'intrus

Le problème de savoir si un intrus peut déduire ou non un terme à partir d'un ensemble de termes est-il décidable ?

Déductibilité

Un terme u est déductible d'un ensemble $T = \{t_1, \ldots, t_n\}$, noté $T \vdash u$, s'il existe un terme C tel que $C[t_1, \ldots, t_n] =_E u$.

La théorie initiale est trop complexe pour obtenir un résultat !

Deuxième Résultat : Décidabilité

Décidabilité de la capacité de calcul de l'intrus

Le problème de savoir si un intrus peut déduire ou non un terme à partir d'un ensemble de termes est-il décidable ?

Déductibilité

Un terme u est déductible d'un ensemble $T = \{t_1, \ldots, t_n\}$, noté $T \vdash u$, s'il existe un terme C tel que $C[t_1, \ldots, t_n] =_E u$.

La théorie initiale est trop complexe pour obtenir un résultat !

Deuxième Résultat : Décidabilité

On simplifie la théorie équationelle :

- On supprime les symboles AC.
- On enlève l'équation d'homomorphisme du chiffrement.

Théorème

Avec cette théorie équationelle légèrement simplifiée, le problème :

$$\text{Soit } T = \{t_1, \ldots, t_n\} \text{ et un terme } M : T \overset{?}{\vdash} M$$

est décidable.

Deuxième Résultat : Décidabilité

On simplifie la théorie équationelle :

- On supprime les symboles AC.
- On enlève l'équation d'homomorphisme du chiffrement.

Théorème

Avec cette théorie équationelle légèrement simplifiée, le problème :

$$\textit{Soit } T = \{t_1, \ldots, t_n\} \textit{ et un terme } M : T \overset{?}{\vdash} M$$

est décidable.

Troisième Résultat : Application de ProVerif

ProVerif : Outil de vérification automatique des protocoles, développé par B. Blanchet.

Seule la théorie simplifiée est supportée.

Corrompus	0 Votant	1 Votant	2 Votants
Tous honnêtes	✓	✓	✓
Urne	–	–	–
Générateur de reçus	✓	✓	✓
Urne et Générateur	–	–	–

Conclusion

Rappel des contributions

- Un résultat de confidentialité sur un protocole utilisé.
- Un résultat de décidabilité.
- Des résultats avec des hypothèses de corruption supplémentaires.

Que reste-t-il à faire ?

- Une démonstration à polir.
- Des cas de corruption à traiter dans la théorie complète.
- Développer un outil (automatique) pour analyser plus globalement les protocoles de vote. (Thèse)
- Analyser d'autres protocoles, à la main ou avec un tel outil.

Conclusion

Rappel des contributions

- Un résultat de confidentialité sur un protocole utilisé.
- Un résultat de décidabilité.
- Des résultats avec des hypothèses de corruption supplémentaires.

Que reste-t-il à faire ?

- Une démonstration à polir.
- Des cas de corruption à traiter dans la théorie complète.
- Développer un outil (automatique) pour analyser plus globalement les protocoles de vote. (Thèse)
- Analyser d'autres protocoles, à la main ou avec un tel outil.

Questions

Merci de votre attention.