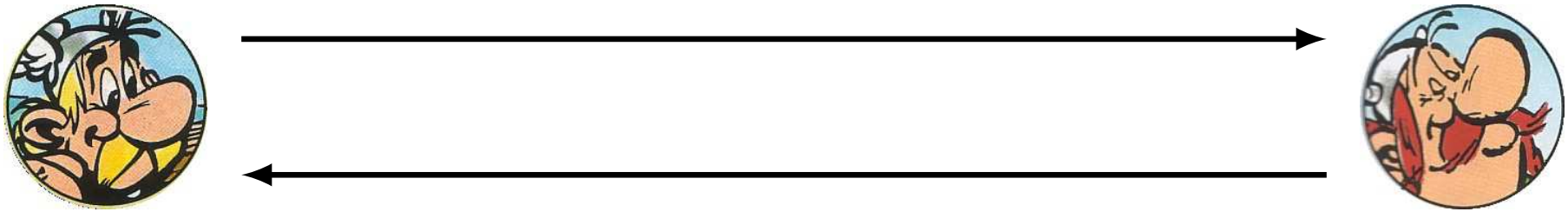
Vérification de protocoles et programmes cryptographiques

Bruno Blanchet

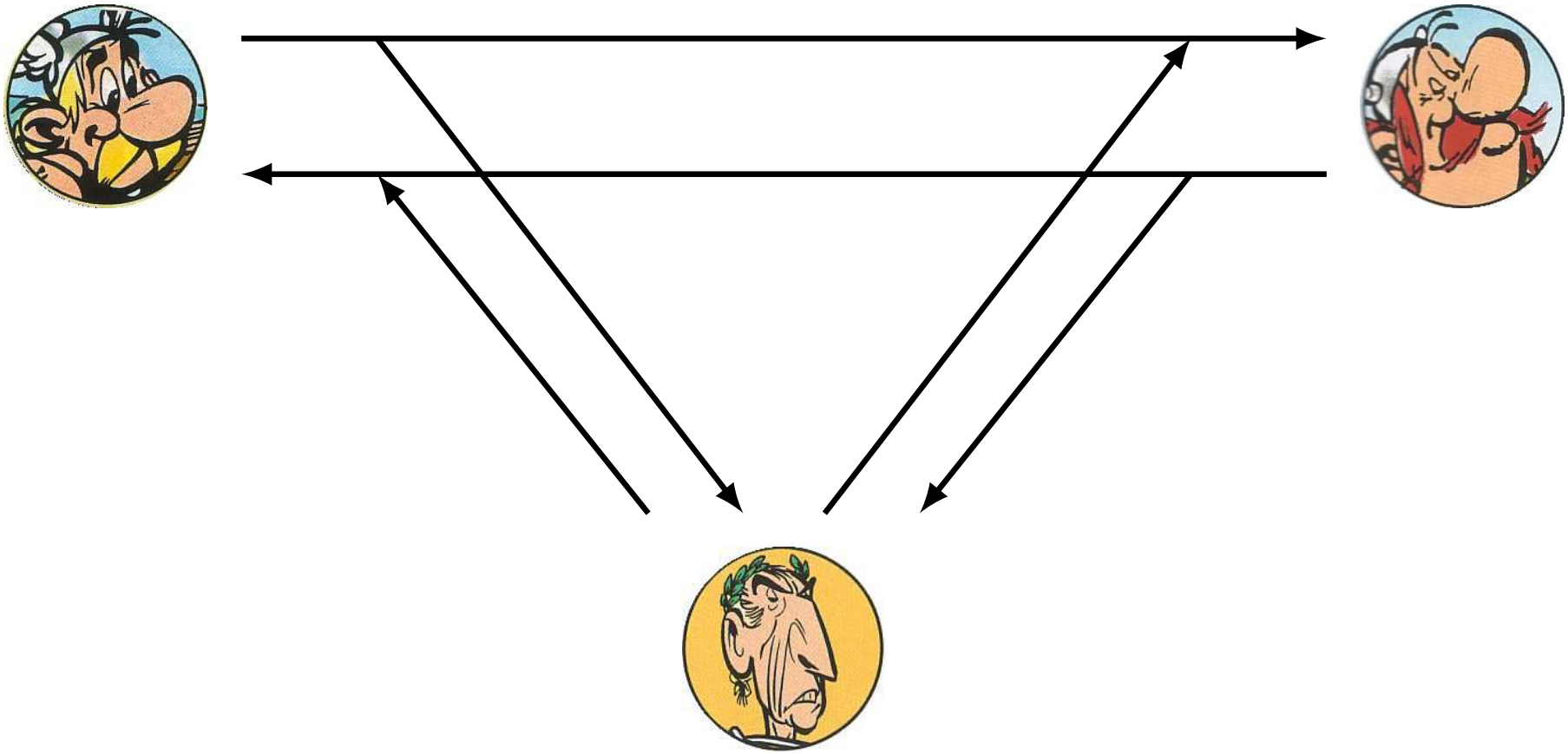
EPI Prosecco
INRIA Paris-Rocquencourt
Bruno.Blanchet@inria.fr

Rencontre Inria - Industrie "Télécoms du futur"
Table ronde "Sécurité des Réseaux et Contenus"
Novembre 2014

Protocole et attaquant



Protocole et attaquant



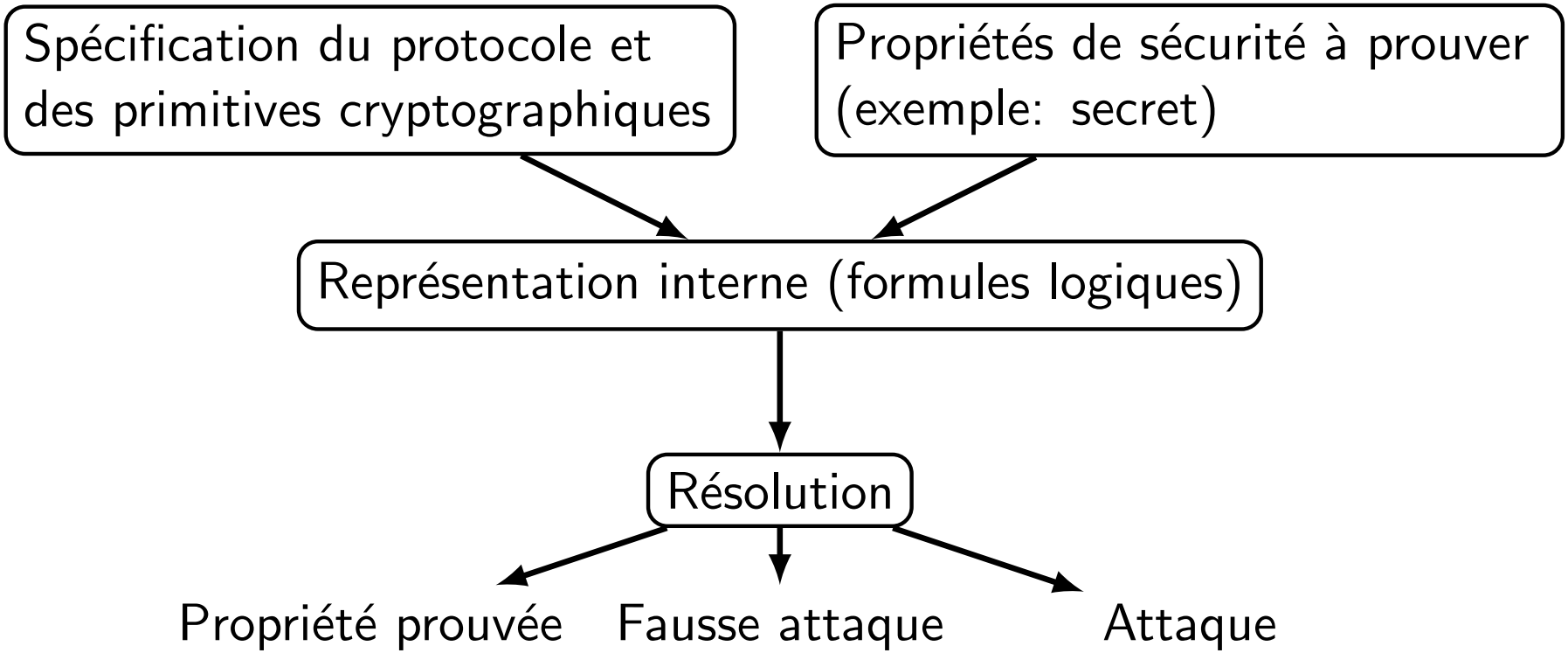
Utiliser la cryptographie pour protéger les données échangées

Intérêt des méthodes formelles

- La conception des protocoles est délicate.
  - Nombreuses attaques dans des protocoles publiés ou utilisés en pratique.
- Les erreurs de sécurité n'apparaissent qu'en présence d'un attaquant.
  - $\Rightarrow$ elles ne sont pas détectées par les tests.
- Utiliser les méthodes formelles pour vérifier les protocoles.
  - Exploration exhaustive de tout ce que l'attaquant peut faire.
    - (dans une certaine classe d'attaques)
  - Découverte d'attaques
  - Preuve de sécurité

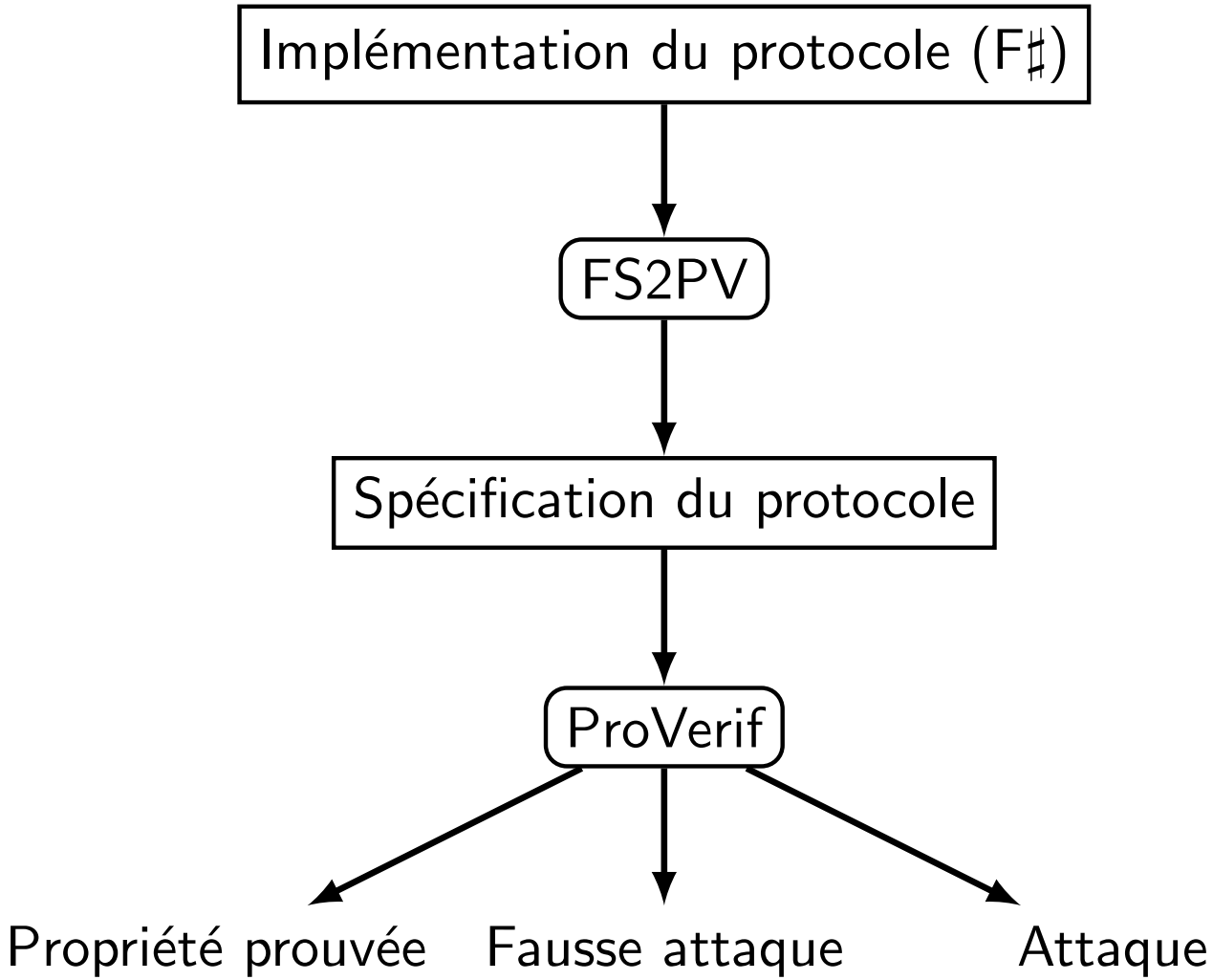
Vérification de spécifications de protocoles

- ProVerif, `http://proverif.inria.fr`

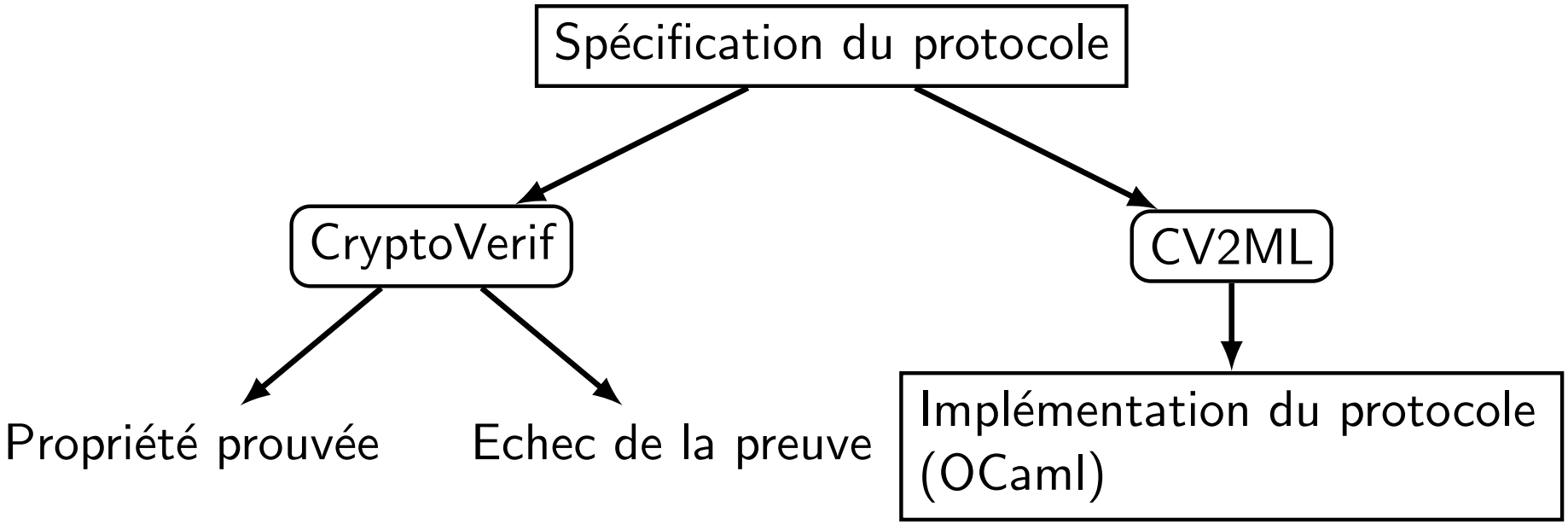


- CryptoVerif, `http://cryptoverif.inria.fr`

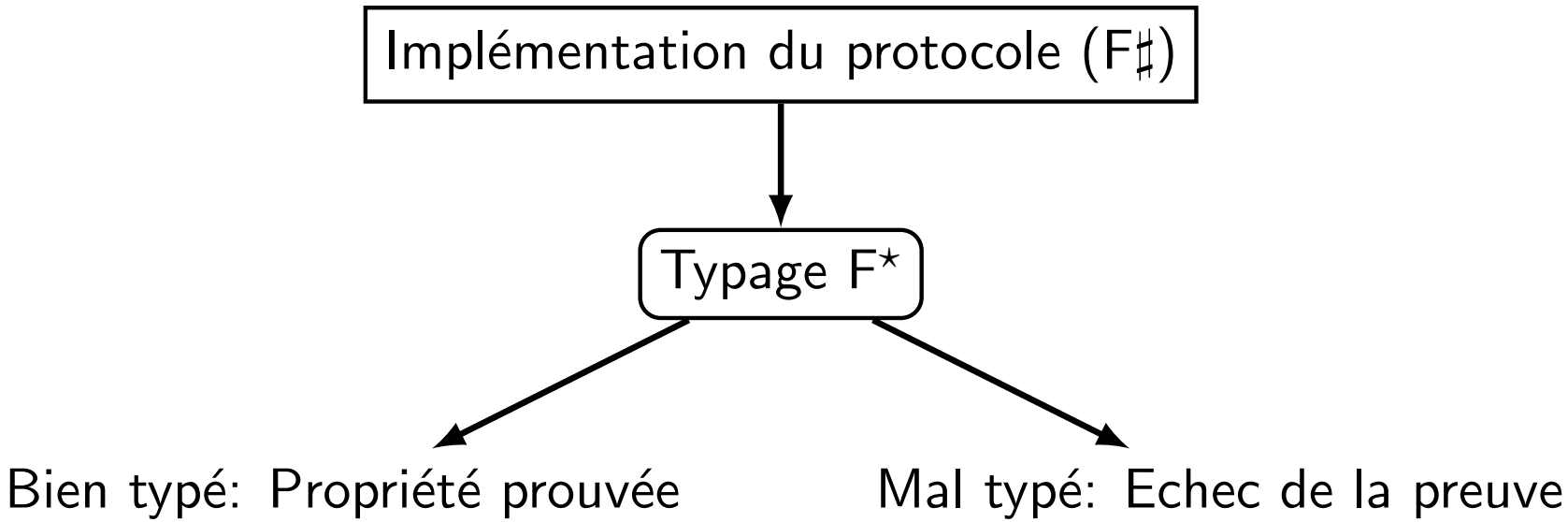
Vérification d'implémentations de protocoles



Vérification d'implémentations de protocoles



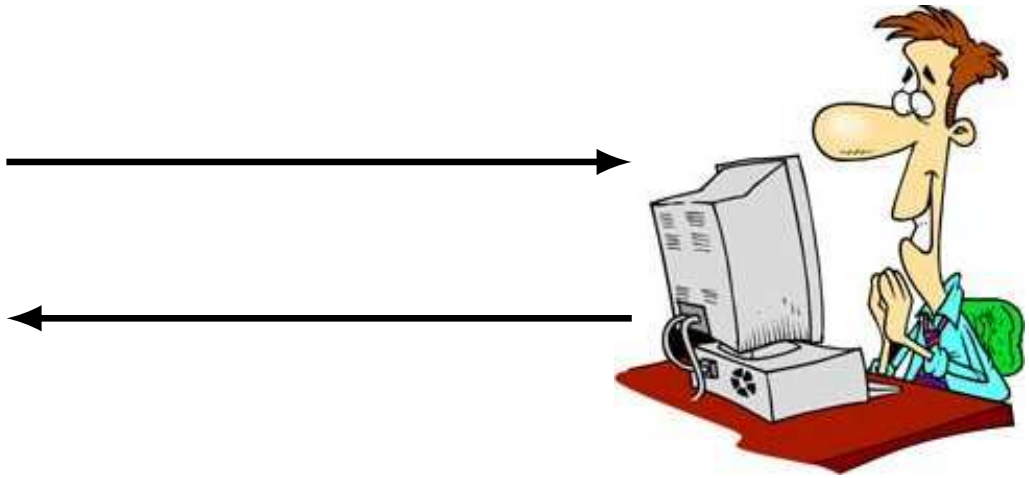
Vérification d'implémentations de protocoles



`http://research.microsoft.com/fstar/`
Application à TLS: `http://www.mitls.org`

Vérification de modules de sécurité

HSM picture by Alexander Klink



Start-up Cryptosense, `http://cryptosense.com/`