DEREC - Développement de la cryptographie relativiste

André Chailloux

Développement de la cryptographie relativiste

DEREC

Programme : ANR CE39

Édition : 2016

Instrument : JCJC

Contact : andre.chailloux@inria.fr

COORDINATEUR : André Chailloux **PARTENAIRES : Inria de Paris**

Résumé (3 lignes max) :
Le but de DEREC est de développer la cryptographie relativiste, un axe de recherche novateur et innovant, dont l'objectif est d'utiliser un principe de physique relativiste qui implique que l'information ne peut pas être transmise à une vitesse plus grande que celle de la lumière, pour la garantir sécurité informatique à long terme.

CONTEXTE ET OBJECTIFS

La plupart des propositions cryptographiques se basent sur des hypothèses calculatoires et, de ce fait, ne garantissent nullement de sécurité à long terme, et donc rétroactive. Sans pessimisme particulier, on peut affirmer que plusieurs systèmes utilisés aujourd'hui se basant sur de telles hypothèses, seront obsolètes dans les 10 à 30 ans à venir.

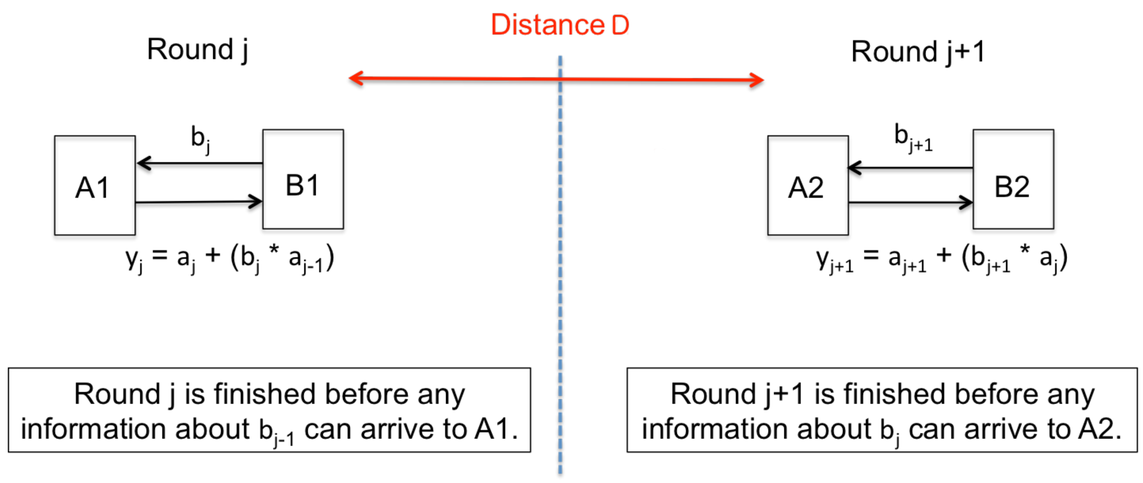
DEREC est un projet unique en son genre qui propose de créer des systèmes avec une sécurité inconditionnelle, et avec du matériel accessible aujourd'hui. Le projet se concentre en particulier sur les systèmes d'identification ainsi que d'autres applications multi utilisateurs comme les systèmes de vote électronique et les systèmes d'enchères en ligne.

MÉTHODOLOGIE ET RÉSULTATS

Méthodologie : Les protocoles cryptographiques ont éte très peu étudiés. Nous avons tout d'abord fait un état des lieu des possibilités de cette idée. Nous avons pu déterminer des premiers axes de recherche, et avons décidé de nous focaliser sur 3 briques de base, essentielles pour des applications futures: la mise en gage de bit, le transfert oublieux et les protocoles d'identification.

Résultats majeurs du projet : Le projet est encore jeune et vient de finir sa première année. Néanmoins, nous avons déjà montré 2 résultats, accompagnés chacun d'une publication concernant les applications de ces systèmes relativistes pour les protocoles zero-knowledge ainsi qu'une étude sur l'efficacité des protocoles de mise-en-gage de bit.

.



FIGURE

L'idée de base est de séparer 2 agents A et B en plusieurs sous-agents dans différentes locations. Les contraintes spatio-temporelles, couplées à des protocoles multi rondes avancées, ouvrent de nouvelles perspectives pour la sécurité à long terme

VALORISATION ET PERSPECTIVES

Les résultats obtenus ont donné lieu à 2 publications

A.Chailloux, A. Leverrrier : Relativistic (or 2-Prover 1-Round) Zero-Knowledge Protocol for NP Secure Against Quantum Adversaries. EUROCRYPT 2017.
R. Bricout, A.Chailloux : Recursive Cheating Strategies for the Relativistic FQ Bit Commitment Protocol, MDPI 2017

Perspectives : Nous avons étudié certaines primitives cryptographiques dans le cadre relativiste nécessaires pour la création de systèmes cryptographiques plus complexes. Nous devons encore poursuivre cette étude. Nous regardons aussi déjà les besoins en matériel (horloges GPS notamment) pour mener à bien les implémentations. Nous avons budgété des équipements en 2017 pour cela. L'arrivée d'un nouvel étudiant travaillant sur le sujet va également considérablement accélérer notre démarche.