CHRONOS

Chronographie Sécurisée

ACI Sécurité 2003-2006

Plan

- Présentation de l'ACI
- Qu'est ce que l'horodatage?
- Présentation d'un système mono serveur
- Perspectives

Les trois équipes du projet

- **Mont de Marsan** (Laboratoire LIUPPA Equipe CSySEC)
  - Alban Gabillon
  - Kaouther Blibech
- **Toulon** (Laboratoire STIC-ISITV)
  - Sami Harari
  - Laurent Poinsot
- **Marseille**
  - Alexis Bonnecaze (LIF)
  - Pierre Liardet (LATP)

Missions de Chronos

Développer la recherche dans le domaine de l'horodatage de documents électroniques :

- Analyser les techniques existantes
- Proposer de nouvelles voies de recherches
- Concevoir de nouveaux protocoles
  - *Mono serveurs*
  - *Multi serveurs*

L'horodatage électronique

- **Authentification de documents électroniques**
  - Signature : qui est le propriétaire?
  - Horodatage : dater le document

- **Horodatage**
  - D a été créé dans un intervalle de temps $[t_0,t_1]$:

  Datation absolue
  - D a été créé après D_0 et avant D_1 :

  Datation relative

- **Principales applications**
  - Commerce électronique, votes électroniques, sécurité, …

Fonctionnement

- Alice construit l'empreinte h(D)

- Alice envoie h(D) à **l'autorité d'horodatage** (TSA)

- La TSA renvoie à Alice le certificat d'horodatage, appelé cachet, qui a été construit par lui grâce à un **protocole d'horodatage** particulier

- Le vérifieur se procure D et le cachet et utilise le **protocole de vérification** associé au protocole d'horodatage

La TSA doit être fiable, de confiance et disponible

Les risques

- **Les risques naturels**
  - Défaillances matérielles ou logicielles
- **Les fraudes**
  - Déni de service
  - Man in the middle
  - Perte de contrôle du serveur
  - Compromission de la clé

Eviter les attaques malveillantes

- Pendant la construction du cachet
  - Empêcher l'autorité de tricher
- Modification d'un cachet existant
  - Empêcher de construire un faux cachet a partir de cachets corrects

Deux architectures

- **Les systèmes monoserveurs**

L'horodatage est effectué par une seule machine (les systèmes existants sont monoserveurs)

- **Les systèmes multiserveurs**

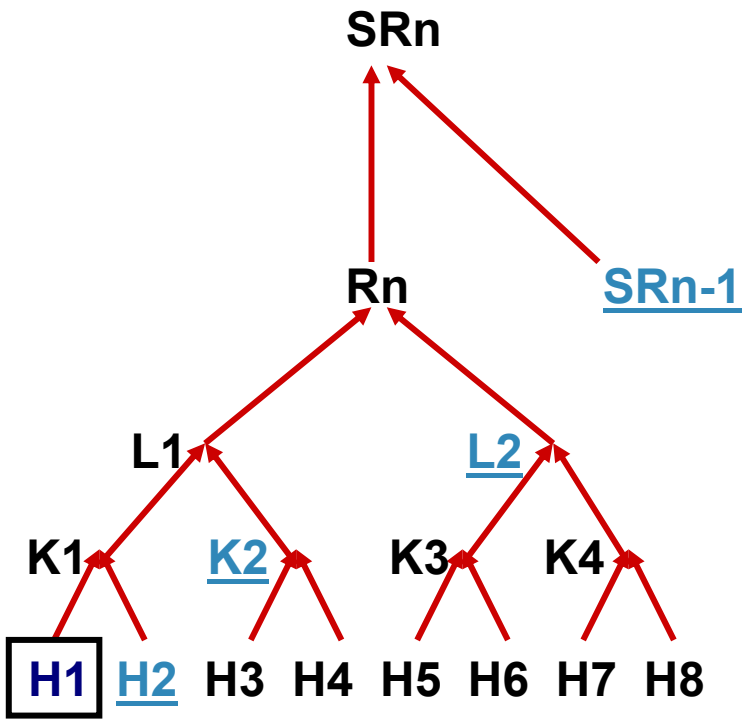
L'horodatage est effectué en parallèle par n machines appartenant à des entités administrativement indépendantes

Les techniques actuelles

- **Cachet certifié** :
  - Exemple : La Poste
  - Il faut faire confiance à la société, tiers de confiance

- **Cachet prouvable** :
  - Exemple : Timesec, Cuculus, PKITS,…
  - Il existe une preuve que le cachet est correct
  - Utilisent des ***schémas de liaison***

S= (t, SRn, Hi to SRn, SRn-1)



Arbre de Merkle

Le nombre de requêtes Dans le tour doit être une puissance de 2.

Apports de Chronos :

- Monoserveurs
  - Utilisation de skiplist à la place d'arbre de Merkle pour créer un schéma de liaison
- Multiserveurs
  - Concept k parmi n
  - Utilisation de nouvelles primitives cryptographiques (EC, pairings) permettant
    - Un petit cachet
    - L'absence d'interaction entre serveurs

Les Skip lists (mono serveurs)

- Structure de données (William Pugh, 1989).
- Alternative aux arbres binaires, arbres équilibrés, …
- Permet insertion, suppression et recherche d'éléments.

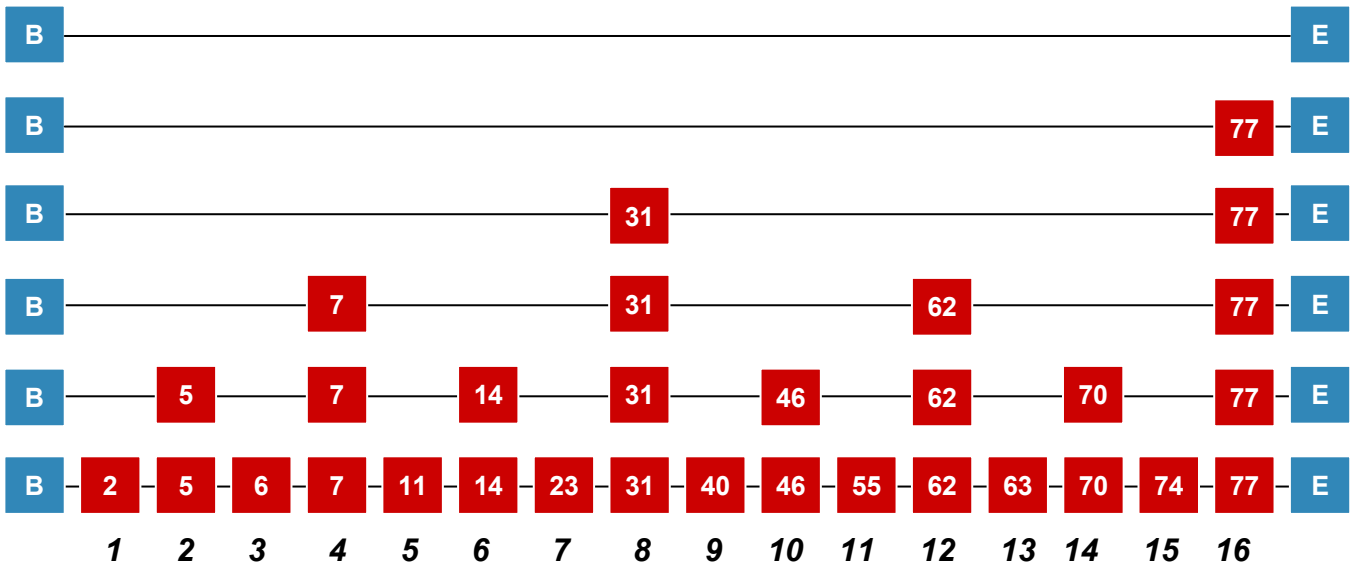
Pour le time stamping

1. Prouver qu'un élément appartient à un tour donné
2. Prouver sa position dans la liste

Skip list vs *Merkle tree* :

- Implantation facile indépendamment du nombre de requêtes
- Ordre des requêtes pris en compte
- Taille de cachet inférieure
- Nombre de calculs de hachés inférieur

Perfect Skip Lists



Perfect Skip List

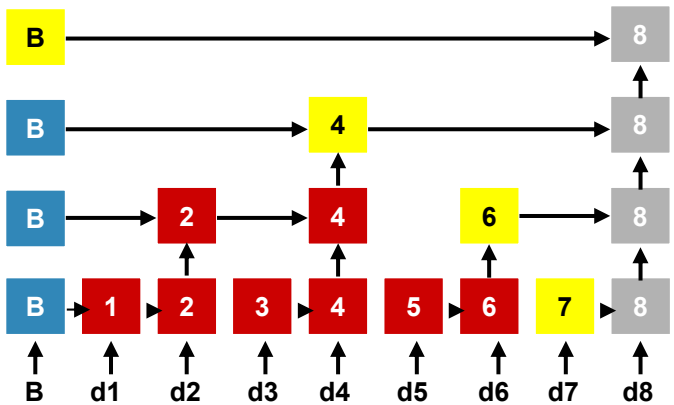
- hauteur d'un élément :

  i si l'indice est multiple de 2^i.

Chronos Timestamping

Calcul de l'accusé de réception pour d8 :

Head proof = nœuds jaunes

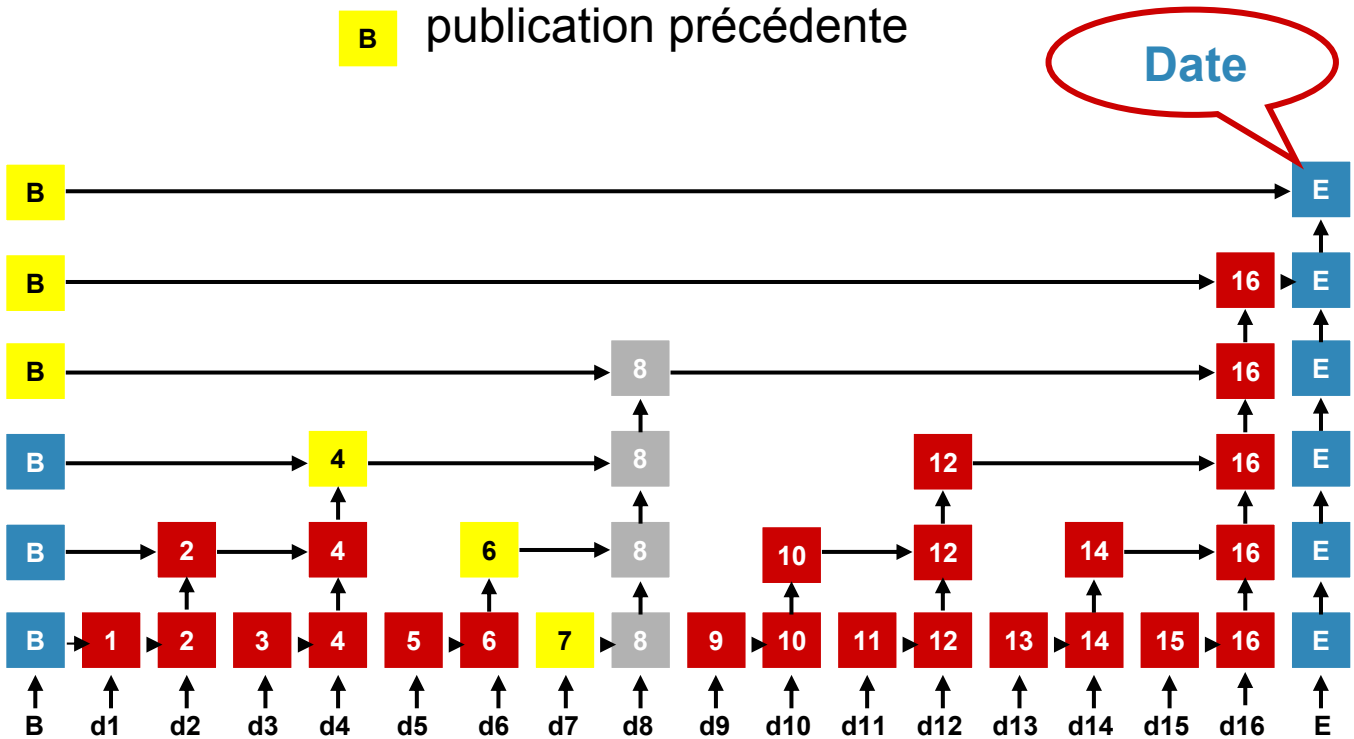


Exemple :

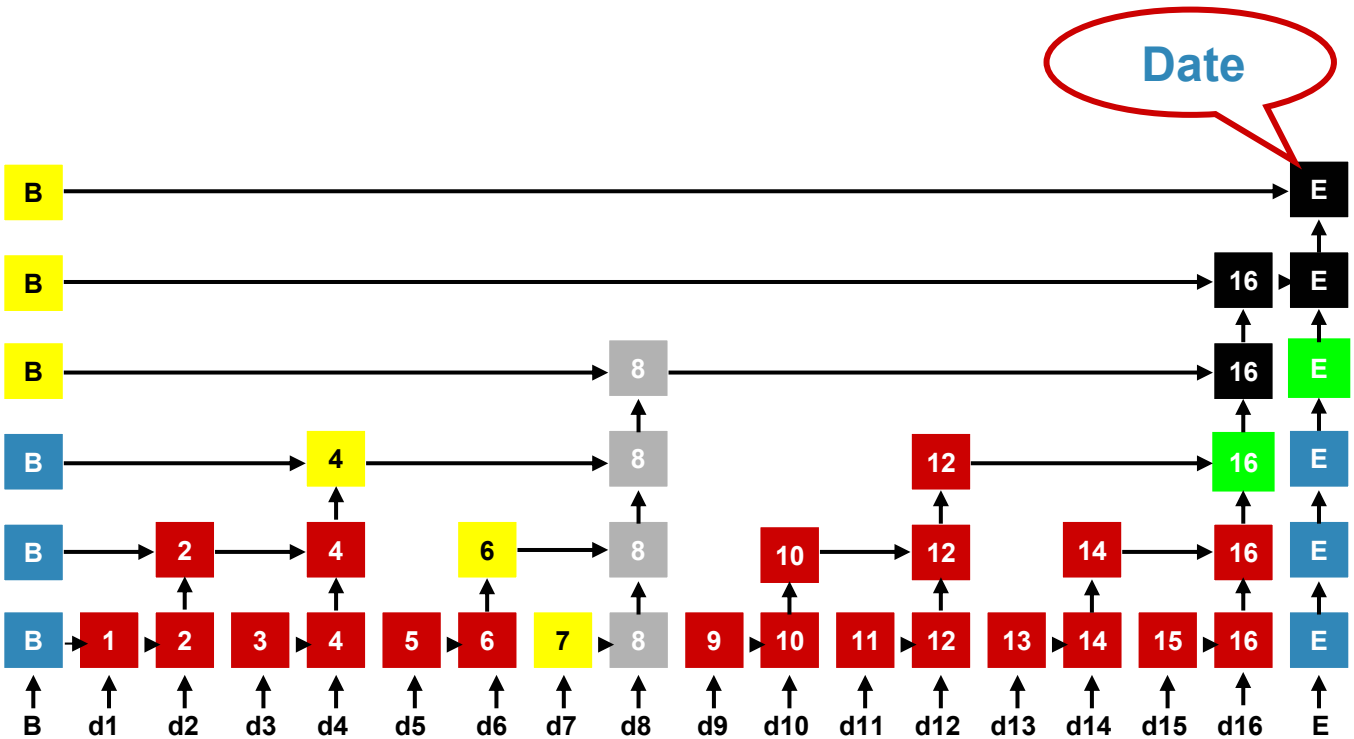
16 requêtes dans le tour

E est publiée avec la date

B publication précédente



Calcul du cachet



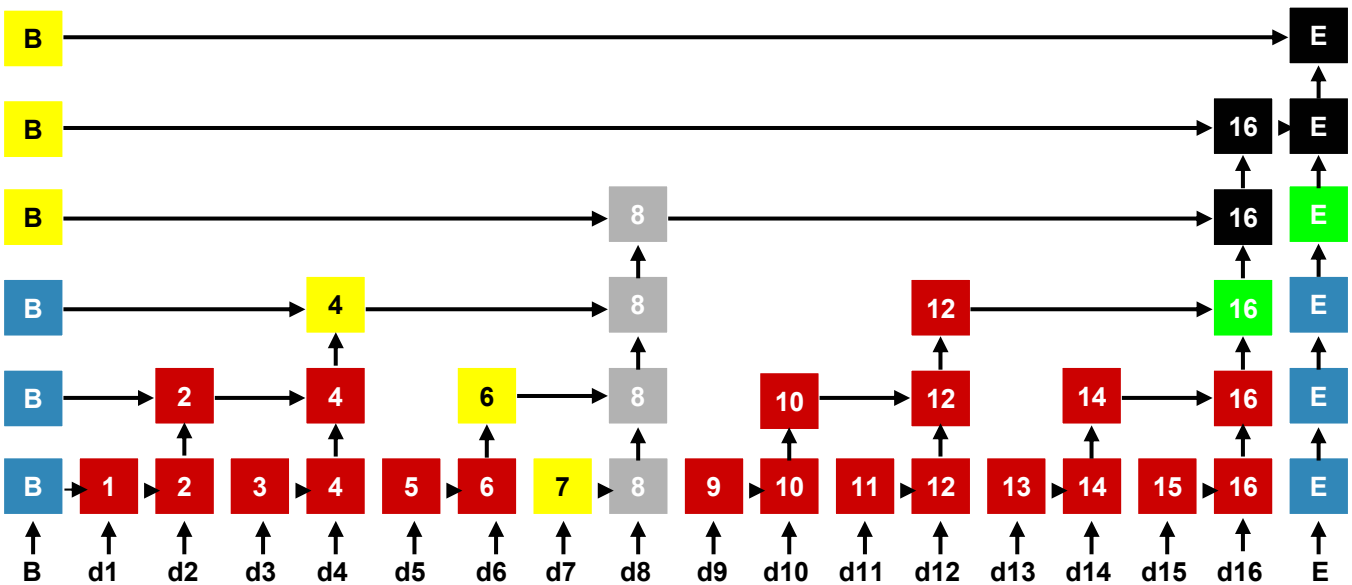
Index = 8

Head proof = nœuds jaunes

Tail proof = nœuds verts

Chronos Timestamping,

1. Ordre des soumissions préservé
2. Aucune contrainte sur le nombre de requêtes
3. Absence de Trapdoor (Accumulators)



Chronos Skip List : Prototype

Published values

TS : Thu September 15 11:29:49 2005

Auth : c729e70ba4f1c303b2a39db0509274e8

Timestamping Token

Index : 8

Head : [92ff95028bfdbeff4397312482fb074d,
230c54f3757760cb7af1ee70b6d6ef72,
996148165ff8df477bcf1698a5e00476, Begin]

Tail : [a5c701bd64f910e9da729397ba982eaa,
192c99d4bb0bfd538b925910bcef670f]

Perspectives

- Adaptation des skip lists pour un schéma multiserveurs
- Implantation du système multiserveurs utilisant des multisignatures courtes
- Recherche de primitives cryptographiques adaptées à l'horodatage

Contributions de Chronos

- **Etat de l'art :**
  - Congrès *INFORSID*, 25 Mai 2004, Biarritz.
  - *Technique et Science Informatiques*, (TSI, Hermes), 30 pages, 2005 à paraître.

Contributions de Chronos

- **Systèmes mono serveur :**
  - *SWS05 12th ACM Conference on Computer Security, Fairfax.*
  - *Inforsid 2005, Grenoble.*
  - *GESTS (Global Engineering, Science and Technology Society).*
- **Systèmes multi serveurs :**
  - *SAR05.*
  - *IEEE-SITIS.*
- **Soumis :**
  - *Annals of telecom* (15 pages).
  - *ICC06* (6 pages).