Vers un marquage spatio-temporel des documents électroniques

Philippe Balbiani
Institut de recherche en informatique de Toulouse

Cryptographie à clé publique

- Nature du problème à résoudre
  - Répondre, relativement à un document électronique donné, aux questions suivantes :
    - Qui a pu l'écrire ?
    - Qui va pouvoir le lire ?
- Solution
  - Cryptographie à clé publique

Marquage temporel

- Nature du problème à résoudre
  - Répondre, relativement à un document électronique donné, aux questions suivantes :
    - Quand a-t-il été écrit ?
    - Quand a-t-il existé sous sa forme présente ?
- Solution
  - Marquage temporel

Marquage temporel

- Une solution simpliste
  - Alice possède un certain document électronique x
  - f désigne une fonction à sens unique
  - σ_{AH} désigne la fonction de signature de l'autorité horodatrice
    - Alice calcule $y=f(x)$ et envoie $\langle ID_A,y\rangle$, où ID_A est l'identificateur d'Alice, à l'autorité horodatrice
    - L'autorité horodatrice calcule $z=\sigma_{AH}(\langle y,t_{AH}\rangle)$, où t_{AH} est l'heure à laquelle elle reçoit $\langle ID_A,y\rangle$, et envoie z au client identifié par ID_A

Marquage temporel

- Principes
  - La durée des communications à destination de l'autorité horodatrice est la plus courte possible
  - Quelque soit l'endroit duquel Alice envoie $\langle ID_A, y \rangle$, nous supposerons que l'autorité horodatrice reçoit $\langle ID_A, y \rangle$ dans un temps extrêmement petit
  - L'autorité horodatrice doit pouvoir recevoir en un temps proche de *0* les messages qui lui sont envoyés, quelque soit l'endroit duquel ces messages partent

Marquage temporel

- Un protocole horodateur distribué
  - G désigne un générateur pseudo-aléatoire
  - n désigne un nombre entier positif
    - Alice calcule $y=f(x)$ et envoie $\langle ID_A,y\rangle$ aux autorités horodatrices identifiées par $ID_1=G^1(y)$, …, $ID_n=G^n(y)$
    - Pour tout $i\in\{1,\ldots,n\}$, l'autorité horodatrice identifiée par ID_i calcule $z_i=\sigma_{AHi}(\langle y,t_{AH,i}\rangle)$, où $t_{AH,i}$ est l'heure à laquelle elle reçoit $\langle ID_A,y\rangle$, et envoie z_i au client identifié par ID_A

Marquage temporel

- Un protocole horodateur chaîné
  - Alice calcule $y=f(x)$ et envoie $\langle ID_A,y\rangle$ à l'autorité horodatrice
  - En réponse à la requête $\langle ID_k,y_k\rangle$, l'autorité horodatrice calcule $z_k=\sigma_{AH}(\langle ID_k,y_k,t_{AH,k},k,L_k\rangle)$, où $t_{AH,k}$ est l'heure à laquelle elle reçoit $\langle ID_k,y_k\rangle$, envoie z_k au client identifié par ID_k et envoie ID_k au client identifié par ID_{k-1}
  - $L_k=\langle ID_{k-1},y_{k-1},t_{AH,k-1},k-1,f(L_{k-1})\rangle$

Marquage spatial

- Nature du problème à résoudre
  - Répondre, relativement à un document électronique donné, aux questions suivantes :
    - Où a-t-il été écrit ?
    - Où a-t-il existé sous sa forme présente ?
- Solution
  - Marquage spatial

Marquage spatial

- Une solution simpliste
  - Alice possède un certain document électronique x
  - f désigne une fonction à sens unique
  - σ_{AT} désigne la fonction de signature de l'autorité topographieuse
    - Alice calcule $y=f(x)$ et envoie $\langle ID_A, y \rangle$ à l'autorité topographieuse
    - L'autorité topographieuse calcule $z=\sigma_{AT}(\langle y, s_{AT} \rangle)$, où s_{AT} est l'endroit duquel elle reçoit $\langle ID_A, y \rangle$, et envoie z au client identifié par ID_A

Marquage spatial

- Principes
  - La distance des communications à destination de l'autorité topographieuse est la plus courte possible
  - Quelque soit l'heure à laquelle Alice envoie $\langle ID_A, y \rangle$, nous supposerons que l'autorité topographieuse reçoit $\langle ID_A, y \rangle$ dans un espace extrêmement petit
  - L'autorité topographieuse doit pouvoir recevoir en un espace proche de *0* les messages qui lui sont envoyés, quelque soit l'heure à laquelle ces messages partent

Marquage spatial

- Un protocole topographieur distribué
  - G désigne un générateur pseudo-aléatoire
  - n désigne un nombre entier positif
    - Alice calcule $y=f(x)$ et envoie $\langle ID_A,y\rangle$ aux autorités topographieuses identifiées par $ID_1=G^1(y)$, …, $ID_n=G^n(y)$
    - Pour tout $i\in\{1,\ldots,n\}$, l'autorité topographieuse identifiée par ID_i calcule $z_i=\sigma_{ATi}(\langle y,s_{AT,i}\rangle)$, où $s_{AT,i}$ est l'endroit duquel elle reçoit $\langle ID_A,y\rangle$, et envoie z_i au client identifié par ID_A

Marquage spatial

- Un protocole topographieur chaîné
  - Alice calcule $y=f(x)$ et envoie $\langle ID_A,y\rangle$ à l'autorité topographieuse
  - En réponse à la requête $\langle ID_k,y_k\rangle$, l'autorité topographieuse calcule $z_k=\sigma_{AT}(\langle ID_k,y_k,s_{AT,k},k,L_k\rangle)$, où $s_{AT,k}$ est l'endroit duquel elle reçoit $\langle ID_k,y_k\rangle$, envoie z_k au client identifié par ID_k et envoie ID_k au client identifié par ID_{k-1}
  - $L_k=\langle ID_{k-1},y_{k-1},s_{AT,k-1},k-1,f(L_{k-1})\rangle$

Marquage spatio-temporel

- Nature du problème à résoudre
  - Répondre, relativement à un document électronique donné, aux questions suivantes :
    - Quand et où a-t-il été écrit ?
    - Quand et où a-t-il existé sous sa forme présente ?
- Solution
  - Marquage spatio-temporel

Marquage spatio-temporel

- Des solutions mauvaises et une bonne solution
  - Attention ! Toute composition ne constitue pas forcément une solution à notre problème
    - Alice calcule $y=f(x)$ et envoie $\langle ID_A,y\rangle$ aux autorités horodatrice et topographieuse
    - L'autorité horodatrice calcule $z_{AH}=\sigma_{AH}(\langle y,t_{AH}\rangle)$, où t_{AH} est l'heure à laquelle elle reçoit $\langle ID_A,y\rangle$, et envoie z_{AH} au client identifié par ID_A
    - L'autorité topographieuse calcule $z_{AT}=\sigma_{AT}(\langle y,s_{AT}\rangle)$, où s_{AT} est l'endroit duquel elle reçoit $\langle ID_A,y\rangle$, et envoie z_{AT} au client identifié par ID_A

Marquage spatio-temporel

- Des solutions mauvaises et une bonne solution
  - D'autres compositions sont possibles
    - Alice calcule $y=f(x)$ et envoie $\langle ID_A, y \rangle$ à l'autorité horodatrice
    - L'autorité horodatrice calcule $z_{AH}=\sigma_{AH}(\langle y, t_{AH} \rangle)$, où t_{AH} est l'heure à laquelle elle reçoit $\langle ID_A, y \rangle$, et envoie $\langle ID_A, z_{AH} \rangle$ à l'autorité topographieuse
    - L'autorité topographieuse calcule $z_{AT}=\sigma_{AT}(\langle z_{AH}, s_{AT} \rangle)$, où s_{AT} est l'endroit duquel elle reçoit $\langle ID_A, z_{AH} \rangle$, et envoie z_{AT} au client identifié par ID_A

Marquage spatio-temporel

- Des solutions mauvaises et une bonne solution
  - D'autres compositions sont possibles
    - Alice calcule $y=f(x)$ et envoie $\langle ID_A, y \rangle$ à l'autorité topographieuse
    - L'autorité topographieuse calcule $z_{AT}=\sigma_{AT}(\langle y, s_{AT} \rangle)$, où s_{AT} est l'endroit duquel elle reçoit $\langle ID_A, y \rangle$, et envoie $\langle ID_A, z_{AT} \rangle$ à l'autorité horodatrice
    - L'autorité horodatrice calcule $z_{AH}=\sigma_{AH}(\langle z_{AT}, t_{AH} \rangle)$, où t_{AH} est l'heure à laquelle elle reçoit $\langle ID_A, z_{AT} \rangle$, et envoie z_{AH} au client identifié par ID_A

Marquage spatio-temporel

- Principes
  - La durée des communications à destination de l'autorité horodatrice est la plus courte possible
  - La distance des communications à destination de l'autorité topographieuse est la plus courte possible

Problèmes ouverts

- Des protocoles horodateurs ont été définis qui sont basés sur les arbres binaires ou les accumulateurs à sens unique
  - Est-il possible de définir des protocoles topographieurs basés sur les mêmes principes ?
- Certains protocoles cryptographiques ne seraient d'aucune utilité si les documents électroniques qu'ils traitent n'étaient marqués temporellement
  - Quelle utilité peut avoir un protocole cryptographique dont les documents électroniques qu'il traite sont marqués spatialement ?
- Applications du marquage spatio-temporel ?