Vers un marquage spatio-temporel des documents électroniques

Philippe Balbiani

Université Paul Sabatier
Institut de recherche en informatique de Toulouse
31062 Toulouse Cedex 9, France

Résumé L'accroissement du volume des informations qui sont conservées dans les systèmes informatiques ou échangées à travers les réseaux exige de pouvoir déterminer quand tel ou tel document électronique a été modifié pour la dernière fois. A cet effet, des protocoles horodateurs ont été définis qui ont pour rôle de marquer les documents électroniques d'une estampille qui atteste leur existence à une heure donnée. Mais l'avènement des systèmes informatiques et des réseaux exige également de pouvoir déterminer où tel ou tel document électronique a été modifié pour la dernière fois. En vue de cela, nous définissons des protocoles topographieurs qui ont pour rôle de marquer les documents électroniques d'une estampille qui atteste leur existence à un endroit donné. Au regard de la loi, pour qu'un acte authentique électronique fasse pleine foi de la convention qu'il enferme, il est nécessaire de pouvoir déterminer quand et où il a été dressé. A cet égard, nous examinons comment la composition des protocoles horodateurs et topographieurs évoqués ci-dessus permet de marquer les documents électroniques d'une estampille qui atteste leur existence à une heure donnée à un endroit donné.

Mots-clés : Sécurité informatique, protocoles horodateurs, protocoles topographieurs, marquage spatio-temporel.

1 Introduction

Le but d'un système cryptographique est principalement d'assurer l'intégrité et la confidentialité des données échangées par l'entremise de voies de communication susceptibles d'espionnage. Jusqu'à récemment, les seules questions auxquelles la cryptographie se prévalait de répondre étaient, relativement à un document électronique donné, les suivantes :

- qui a pu l'écrire,
- qui va pouvoir le lire.

Une exigence évidente pour la sécurité des systèmes informatiques et des réseaux, et qui a fait l'objet de nombreuses recherches, est qu'il soit aussi possible de répondre, relativement à un document électronique donné, à la question suivante :

- quand a-t-il été écrit, i.e. quand a-t-il existé sous sa forme présente.

Haber et Stornetta [12] ont présenté la première réalisation pratique du marquage temporel des documents électroniques. Nous passons en revue sommaire, dans la section 2, chacun des principaux modes de marquage temporel des documents électroniques proposés depuis. Voir [3,6,7,10,11].
Une exigence évidente pour la sécurité des systèmes informatiques et des réseaux, et qui n'a fait l'objet d'aucune recherche, est qu'il soit aussi possible de répondre, relativement à un document électronique donné, à la question suivante :

- où a-t-il été écrit, i.e. où a-t-il existé sous sa forme présente.

A la manière des protocoles horodateurs proposés par Haber et Stornetta, nous présentons la première réalisation pratique du marquage spatial des documents électroniques. Nous passons en revue sommaire, dans la section 3, chacun des principaux modes de marquage spatial des documents électroniques que nous proposons. Par la suite, nous montrons, dans la section 4, comment la composition des protocoles horodateurs et topographieurs étudiés dans les sections 2 et 3 permet de marquer les documents électroniques d'une estampille qui atteste leur existence à une heure donnée à un endroit donné. Pour ce qui est de la section 5, nous y étudions trois applications des protocoles horodateurs et topographieurs. La section 6 clôt notre article par l'évocation de trois problèmes ouverts.

2 Protocoles de marquage temporel

L'accroissement du volume des informations qui sont conservées dans les systèmes informatiques ou échangées à travers les réseaux exige de pouvoir déterminer quand tel ou tel document électronique a été modifié pour la dernière fois. A cet effet, des protocoles horodateurs ont été définis qui ont pour rôle de marquer les documents électroniques d'une estampille qui atteste leur existence à une heure donnée.

2.1 Une solution simpliste

Supposons qu'Alice possède un certain document électronique x et qu'elle souhaite le marquer relativement au temps. Dans le protocole horodateur suivant, étudié par Haber et Stornetta [12], f désigne une fonction à sens unique sur laquelle tous les utilisateurs se sont entendus et 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.

Puisque f est une fonction à sens unique, alors pour tout x, il est facile de calculer y tel que $y = f(x)$ et pour la plupart des y, il est difficile de trouver x tel $x \in f^{-1}(y)$. Puisque σ_{AH} est la fonction de signature de l'autorité horodatrice, alors pour tout x, si l'autorité horodatrice envoie $y = \sigma_{AH}(x)$ à Alice alors Alice sera en mesure de prouver à quiconque lui en fera la demande que y a été calculé par nul autre que l'autorité horodatrice et que son contenu n'a pas été altéré par un tripatouilleur. Le protocole horodateur ci-dessus exige bien-sûr qu'Alice ait la même heure que l'autorité horodatrice. Si t_A est l'heure à laquelle Alice envoie $\langle ID_A, y\rangle$ à l'autorité horodatrice, l'intuition veut que z constitue l'estampille qui atteste l'existence de y, et donc de x, à l'heure t_{AH}. Au regard d'une tierce personne, plus $\parallel t_{AH} - t_A \parallel$ sera proche de 0 et plus z constituera une preuve convaincante de l'existence de x à l'heure t_A. En d'autres termes, dans le protocole horodateur ci-dessus, il est essentiel de supposer que

- la durée des communications à destination de l'autorité horodatrice est la plus courte possible.

Plus précisément, 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. Par principe, donc,

- 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.

Ceci est évidemment possible lorsque la communication à destination de l'autorité horodatrice est réalisée à l'aide d'ondes radioélectriques (ondes courtes, petites ondes ou grandes ondes). La

résolution des problèmes techniques que cette utilisation de la radiocommunication engendre n'empêche pas que l'autorité horodatrice choisisse une heure t_{AH} différente de l'heure à laquelle elle reçoit $\langle ID_A, y\rangle$.

2.2 Un protocole horodateur distribué

Pour rendre impossible toute tromperie quelconque, il suffit de donner à plusieurs autorités horodatrices prises séparément une partie de la besogne liée au marquage temporel de x. Dans le protocole horodateur suivant, étudié par Haber et Stornetta [12], toutes les autorités horodatrices se sont accordées pour utiliser le même générateur pseudo-aléatoire G et le même nombre entier positif n :

- 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 $z_i = \sigma_{AH_i}(\langle y, t_i\rangle)$, où t_i est l'heure à laquelle elle reçoit $\langle ID_A, y\rangle$, et envoie z_i au client identifié par ID_A.

Puisque G est un générateur pseudo-aléatoire et n est un nombre entier positif, alors pour tout x, il est facile de calculer ID_1, ..., ID_n tels que $ID_1 = G^1(x)$, ..., $ID_n = G^n(x)$ et pour la plupart des ID_1, ..., ID_n, il est difficile de trouver x tel que $x \in G^{-1}(ID_1)$, ..., $x \in G^{-n}(ID_n)$. Le protocole horodateur ci-dessus, dans lequel σ_{AH_i} désigne bien-sûr la fonction de signature de l'autorité horodatrice identifiée par ID_i, rend difficile toute tromperie quelconque en autant qu'Alice possède une très faible probabilité de tomber sur n autorités horodatrices toutes ensembles corrompues. Son exécution, toutefois, réclame l'envoi de $\langle ID_A, y\rangle$ au même instant par Alice à n autorités horodatrices.

2.3 Un protocole horodateur chaîné

Dans un autre protocole, Haber et Stornetta [12] proposent de lier par un rapport de dépendance les estampilles que l'autorité horodatrice calculent les unes après les autres :

- 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 $\langle ID_k, y_k\rangle$, et envoie z_k au client identifié par ID_k et ID_k au client identifié par ID_{k-1}.

Le protocole horodateur ci-dessus, dans lequel $L_k = \langle ID_{k-1}, y_{k-1}, t_{AH,k-1}, k-1, f(L_{k-1})\rangle$, rend difficile toute tromperie quelconque. En effet, l'autorité horodatrice peut difficilement choisir une heure $t_{AH,k}$ très différente de l'heure à laquelle elle reçoit $\langle ID_k, y_k\rangle$ sans éveiller les soupçons des clients identifiés par ID_{k-1} et ID_{k+1}. Ceci est d'autant plus vrai que l'autorité horodatrice reçoit, par unité de temps, un grand nombre de requêtes. Si l'autorité horodatrice choisit, en recevant $\langle ID_k, y_k\rangle$, une heure $t_{AH,k}$ très différente de l'heure $t_{AH,k-1}$ qu'elle avait choisie en recevant $\langle ID_{k-1}, y_{k-1}\rangle$ alors elle s'expose à être confondue par tout utilisateur qui chercherait, en réclamant auprès des clients identifiés par ID_{k-1} et ID_{k+1} de connaître z_{k-1} et z_{k+1}, à vérifier l'existence de y_k à l'heure $t_{AH,k}$. Son exécution, toutefois, exige l'insertion dans z_k de l'identificateur du client ayant envoyé la requête $\langle ID_k, y_k\rangle$. Cette exigence, les règles présentes standardisant les conditions de réalisation de la datation des documents électroniques la refusent [1].

3 Protocoles de marquage spatial

Mais l'avènement des systèmes informatiques et des réseaux exige également de pouvoir déterminer où tel ou tel document électronique a été modifié pour la dernière fois. En vue de cela, nous définissons des protocoles topographieurs qui ont pour rôle de marquer les documents électroniques d'une estampille qui atteste leur existence à un endroit donné.

3.1 Une solution simpliste

Supposons qu'Alice possède un certain document électronique x et qu'elle souhaite le marquer relativement à l'espace. A la manière du premier protocole horodateur proposé par Haber et Stornetta, nous proposons le protocole topographieur suivant dans lequel σ_{AT} désigne bien-sûr 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.

Le protocole topographieur ci-dessus exige bien-sûr qu'Alice soit au même endroit que l'autorité topographieuse. Si s_A est l'endroit duquel Alice envoie $\langle ID_A, y\rangle$ à l'autorité topographieuse, l'intuition veut que z constitue l'estampille qui atteste l'existence de y, et donc de x, à l'endroit s_{AT}. Au regard d'une tierce personne, plus $\| s_{AT} - s_A \|$ sera proche de 0 et plus z constituera une preuve convaincante de l'existence de x à l'endroit s_A. En d'autres termes, dans le protocole topographieur ci-dessus, il est essentiel de supposer que

- la distance des communications à destination de l'autorité topographieuse est la plus courte possible.

Plus précisément, 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. Par principe, donc,

- 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.

Ceci est évidemment possible lorsque la communication à destination de l'autorité topographieuse est réalisée à l'aide de supports informatiques (disques durs, disques souples ou disquettes). La résolution des problèmes techniques que cette utilisation de l'informatique engendre n'empêche pas que l'autorité topographieuse choisisse un endroit s_{AT} différent de l'endroit duquel elle reçoit $\langle ID_A, y\rangle$.

3.2 Un protocole topographieur distribué

Pour faire obstacle à toute tromperie quelconque, il suffit de donner à plusieurs autorités topographieuses prises séparément une partie de la besogne liée au marquage spatial de x. A la manière du second protocole horodateur proposé par Haber et Stornetta, nous proposons le protocole topographieur suivant :

- 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 $z_i = \sigma_{AT_i}(\langle y, s_i\rangle)$, où s_i est l'endroit duquel elle reçoit $\langle ID_A, y\rangle$, et envoie z_i au client identifié par ID_A.

Le protocole topographieur ci-dessus, dans lequel σ_{AT_i} désigne bien-sûr la fonction de signature de l'autorité topographieuse identifiée par ID_i, rend difficile toute tromperie quelconque en autant qu'Alice possède une très faible probabilité de tomber sur n autorités topographieuses toutes ensembles corrompues. Son exécution, toutefois, réclame l'envoi de $\langle ID_A, y\rangle$ au même endroit par Alice à n autorités topographieuses.

3.3 Un protocole topographieur chaîné

A la manière du troisième protocole horodateur proposé par Haber et Stornetta, nous proposons le protocole topographieur suivant :

- 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 $\langle ID_k, y_k\rangle$, et envoie z_k au client identifié par ID_k et ID_k au client identifié par ID_{k-1}.

Le protocole topographieur ci-dessus, dans lequel bien-sûr

$$L_k = \langle ID_{k-1}, y_{k-1}, s_{AT,k-1}, k-1, f(L_{k-1})\rangle,$$

rend difficile toute tromperie quelconque. En effet, l'autorité topographieuse peut difficilement choisir un endroit $s_{AT,k}$ très différent de l'endroit duquel elle reçoit $\langle ID_k, y_k\rangle$ sans éveiller les soupçons des clients identifiés par ID_{k-1} et ID_{k+1}. Ceci est d'autant plus vrai que l'autorité topographieuse reçoit, par unité d'espace, un grand nombre de requêtes. Si l'autorité topographieuse choisit, en recevant $\langle ID_k, y_k\rangle$, un endroit $s_{AT,k}$ très différent de l'endroit $s_{AT,k-1}$ qu'elle avait choisie en recevant $\langle ID_{k-1}, y_{k-1}\rangle$ alors elle s'expose à être confondue par tout utilisateur qui chercherait, en réclamant auprès des clients identifiés par ID_{k-1} et ID_{k+1} de connaître z_{k-1} et z_{k+1}, à vérifier l'existence de y_k à l'endroit $s_{AT,k}$. Son exécution, toutefois, exige l'insertion dans z_k de l'identificateur du client ayant envoyé la requête $\langle ID_k, y_k\rangle$. Cette exigence, les règles futures standardisant les conditions de réalisation de la localisation des documents électroniques la refuseront-elles ?

4 Protocoles de marquage spatio-temporel

Au regard de la loi, pour qu'un acte authentique électronique fasse pleine foi de la convention qu'il enferme, il est nécessaire de pouvoir déterminer quand et où il a été dressé. A cet égard, nous examinons comment la composition des protocoles horodateurs et topographieurs étudiés dans les sections 2 et 3 permet de marquer les documents électroniques d'une estampille qui atteste leur existence à une heure donnée à un endroit donné.

4.1 Des solutions mauvaises et une bonne solution

Attention ! Toute composition ne constitue pas forcément une solution à notre problème. Par exemple, le protocole

- 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

dans lequel les exécutions des protocoles étudiés dans les sections 2.1 et 3.1 sont parallèles. Pour ce protocole, z_{AH} atteste l'existence de x à l'heure t_{AH} mais ne parle aucunement de l'endroit auquel x se trouvait à cette heure-là. De plus, z_{AT} atteste l'existence de x à l'endroit s_{AT} mais ne parle aucunement de l'heure à laquelle x se trouvait à cet endroit-là. Par conséquent, ce protocole ne constitue pas une bonne solution au problème du marquage spatio-temporel de x. D'autres compositions sont possibles. Par exemple, le protocole

- 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

dans lequel les exécutions des protocoles étudiés dans les sections 2.1 et 3.1 sont séquentielles. Examinons ce protocole. D'abord, z_{AH} atteste l'existence de x à l'heure t_{AH}. Ensuite, z_{AT} atteste l'existence de z_{AH} à l'endroit s_{AT}. Toutefois, même si la durée du traitement interne de z_{AH} par l'autorité horodatrice, calcul et envoi, est la plus courte possible, le protocole ci-dessus ne constitue pas une bonne solution au problème du marquage spatio-temporel de x. En effet, il exige que l'autorité horodatrice soit au même endroit que l'autorité topographieuse, condition qu'il est difficile d'assurer. D'autres compositions sont possibles. Par exemple, le protocole

- 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

dans lequel les exécutions des protocoles étudiés dans les sections 2.1 et 3.1 sont séquentielles. Examinons ce protocole. D'abord, z_{AT} atteste l'existence de x à l'endroit s_{AT}. Ensuite, z_{AH} atteste l'existence de z_{AT} à l'heure t_{AH}. Plus rapide sera le traitement interne de z_{AT} par l'autorité topographieuse, calcul et envoi, et plus z_{AH} constituera une preuve convaincante de l'existence de x à l'heure t_{AH} à l'endroit s_{AT}. Par conséquent, si

- la durée du traitement interne de z_{AT} par l'autorité topographieuse est la plus courte possible

alors le protocole ci-dessus constitue une bonne solution au problème du marquage spatio-temporel de x. Notons, par ailleurs, qu'il exige que l'autorité topographieuse ait la même heure que l'autorité horodatrice, condition qu'il est facile d'assurer. L'inconvénient de ce protocole simpliste est, bien-sûr, qu'il n'empêche pas que l'autorité topographieuse choisisse un endroit s_{AT} différent de l'endroit duquel elle reçoit $\langle ID_A, y\rangle$ ou que l'autorité horodatrice choisisse une heure t_{AH} différente de l'heure à laquelle elle reçoit $\langle ID_A, z_{AT}\rangle$.

4.2 Des solutions distribuées

Afin d'empêcher le genre de fraude évoqué à la fin de la section 4.1, nous proposons, dans un premier temps, de composer les protocoles étudiés dans les sections 2.1 et 3.1 avec ceux étudiés dans les sections 2.2 et 3.2. Par exemple, le protocole

- 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 $\langle ID_A, z_{AT}\rangle$ aux autorités horodatrices identifiées par $ID_1 = G^1(z_{AT})$, …, $ID_n = G^n(z_{AT})$,

– pour tout $i \in \{1, \ldots, n\}$, l'autorité horodatrice identifiée par ID_i calcule

$$z_{AH,i} = \sigma_{AH_i}(\langle z_{AT}, t_i \rangle),$$

où t_i est l'heure à laquelle elle reçoit $\langle ID_A, z_{AT} \rangle$, et envoie $z_{AH,i}$ au client identifié par ID_A

dans lequel les exécutions des protocoles étudiés dans les sections 2.2 et 3.1 sont séquentielles. Ce protocole rend difficile toute tromperie quelconque en autant que l'autorité topographieuse possède une très faible probabilité de tomber sur n autorités horodatrices toutes ensembles corrompues. Son exécution, toutefois, n'empêche pas que l'autorité topographieuse choisisse un endroit s_{AT} différent de l'endroit duquel elle reçoit $\langle ID_A, y \rangle$. Pour empêcher que l'autorité topographieuse triche, il est nécessaire de distribuer la besogne liée au marquage spatio-temporel de x dès le début de l'exécution du protocole. Dans le protocole

– 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 $z_{AT,i} = \sigma_{AT_i}(\langle y, s_i \rangle)$, où s_i est l'endroit duquel elle reçoit $\langle ID_A, y \rangle$, et envoie $\langle ID_A, z_{AT,i} \rangle$ à l'autorité horodatrice,
– pour tout $i \in \{1, \ldots, n\}$, l'autorité horodatrice calcule $z_{AH,i} = \sigma_{AH}(\langle z_{AT,i}, t_i \rangle)$, où t_i est l'heure à laquelle elle reçoit $\langle ID_A, z_{AT,i} \rangle$, et envoie $z_{AH,i}$ au client identifié par ID_A,

les exécutions des protocoles étudiés dans les sections 2.1 et 3.2 sont séquentielles. Ce protocole rend difficile toute tromperie quelconque en autant qu'Alice possède une très faible probabilité de tomber sur n autorités topographieuses toutes ensembles corrompues. Son exécution, toutefois, réclame l'envoi de $\langle ID_A, y \rangle$ au même endroit par Alice à n autorités topographieuses.

4.3 Des solutions chaînées

Afin d'empêcher le genre de fraude évoqué à la fin de la section 4.1, nous proposons, dans un second temps, de composer les protocoles étudiés dans les sections 2.1 et 3.1 avec ceux étudiés dans les sections 2.3 et 3.3. Par exemple, le protocole

– 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,
– en réponse à la requête $\langle ID_k, y_k \rangle$, l'autorité horodatrice calcule

$$z_{AH,k} = \sigma_{AH}(\langle ID_k, y_k, t_{AH,k}, k, L_k \rangle),$$

où $t_{AH,k}$ est l'heure à laquelle elle reçoit $\langle ID_k, y_k \rangle$, et envoie $z_{AH,k}$ au client identifié par ID_k et ID_k au client identifié par ID_{k-1}

dans lequel les exécutions des protocoles étudiés dans les sections 2.3 et 3.1 sont séquentielles. Ce protocole, dans lequel bien-sûr $L_k = \langle ID_{k-1}, y_{k-1}, t_{AH,k-1}, k-1, f(L_{k-1}) \rangle$, rend difficile toute tromperie quelconque. En effet, l'autorité horodatrice peut difficilement choisir une heure $t_{AH,k}$ très différente de l'heure à laquelle elle reçoit $\langle ID_k, y_k \rangle$ sans éveiller les soupçons des clients identifiés par ID_{k-1} et ID_{k+1}. Son exécution, toutefois, n'empêche pas que l'autorité topographieuse choisisse un endroit s_{AT} différent de l'endroit duquel elle reçoit $\langle ID_A, y \rangle$. Pour empêcher que l'autorité topographieuse triche, il est nécessaire de chaîner la besogne liée au marquage spatio-temporel de x dès le début de l'exécution du protocole. Dans le protocole

– 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

$$z_{AT,k} = \sigma_{AT}(\langle ID_k, y_k, s_{AT,k}, k, L_k \rangle),$$

où $s_{AT,k}$ est l'endroit duquel elle reçoit $\langle ID_k, y_k \rangle$, et envoie $\langle ID_k, z_{AT,k} \rangle$ à l'autorité horodatrice et ID_k au client identifié par ID_{k-1},
– l'autorité horodatrice calcule $z_{AH,k} = \sigma_{AH}(\langle z_{AT,k}, t_{AH,k} \rangle)$, où $t_{AH,k}$ est l'heure à laquelle elle reçoit $\langle ID_k, z_{AT,k} \rangle$, et envoie $z_{AH,k}$ au client identifié par ID_k,

les exécutions des protocoles étudiés dans les sections 2.1 et 3.3 sont séquentielles. Ce protocole, dans lequel bien-sûr $L_k = \langle ID_{k-1}, y_{k-1}, s_{AT,k-1}, k-1, f(L_{k-1}) \rangle$, rend difficile toute tromperie quelconque. En effet, l'autorité topographieuse peut difficilement choisir un endroit $s_{AT,k}$ très différent de l'endroit duquel elle reçoit $\langle ID_k, y_k \rangle$ sans éveiller les soupçons des clients identifiés par ID_{k-1} et ID_{k+1}.

5 Applications

Dans cette section, nous étudions trois applications des protocoles proposés ci-dessus : la datation, la localisation et le marquage spatio-temporel des documents électroniques obtenus par l'intermédiaire de systèmes cryptographiques à clé publique. a désignera la clé personnelle d'Alice et D_a et E_a désigneront ses clés personnelle et publique.

5.1 Datation

De nombreux systèmes cryptographiques à clé publique s'appuient sur l'espoir que l'exponentiation modulaire avec un exposant et un module fixés est une fonction à brèche secrète et certains d'entre eux possèdent la propriété qu'obtenir les textes clairs à partir des textes chiffrés est exactement aussi difficile que de factoriser de grands nombres entiers positifs. L'utilisation de D_a est donc compromise pendant certaines périodes. Considérons un message x et posons $y = D_a(x)$. Si Alice calcule y alors, dès que l'utilisation de D_a est compromise, elle n'est plus en mesure de prouver à quiconque lui en fait la demande que y a été calculé par nul autre qu'elle et que son contenu n'a pas été altéré par un tripatouilleur. C'est pourquoi les clés personnelles des uns et des autres ont des durées d'utilisation limitées. Pour pérenniser la possibilité qu'a Alice de prouver à quiconque lui en fait la demande que $D_a(x)$ a été calculé par nul autre qu'elle et que son contenu n'a pas été altéré par un tripatouilleur, il suffit de marquer $D_a(x)$ d'une estampille qui atteste son existence à une heure différente des heures auxquelles l'utilisation de D_a est compromise. Pour ce faire, nous proposons, à la manière du protocole étudié dans la section 2.1, le protocole suivant :

– Alice calcule $y = D_a(x)$ et envoie $\langle ID_A, y \rangle$ 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.

Nous l'avons dit, z constitue l'estampille qui atteste l'existence de y à l'heure t_{AH}. Si l'heure t_{AH} est différente des heures auxquelles l'utilisation de D_a est compromise alors Alice sera toujours en mesure de prouver à quiconque lui en fait la demande que y a été calculé par nul autre qu'elle et que son contenu n'a pas été altéré par un tripatouilleur. Cette application du marquage temporel des documents électroniques, les règles présentes standardisant les conditions de réalisation de la datation des documents électroniques la mentionnent [1].

5.2 Localisation

De nombreux pays soumettent à un règlement l'importation et l'exportation des moyens de cryptographie et certains d'entre eux n'autorisent sur leur territoire que le stockage d'éléments résultant d'un usage de la cryptographie effectué à l'extérieur de leur territoire. L'utilisation de E_a est donc interdite dans certaines régions. Considérons un message x et posons $y = E_a(x)$. Si Alice calcule y alors, là où l'utilisation de E_a est interdite, Alice n'est plus en mesure de prouver à quiconque lui en fait la demande que y a été calculé pour nul autre qu'elle et que son contenu n'a pas été altéré par un tripatouilleur. C'est pourquoi les clés publiques des uns et des autres ont des espaces d'utilisation limités. Pour universaliser la possibilité qu'a Alice de prouver à quiconque lui en fait la demande que $E_a(x)$ a été calculé pour nul autre qu'elle et que son contenu n'a pas été altéré par un tripatouilleur, il suffit de marquer $E_a(x)$ d'une estampille qui atteste son existence à un endroit différent des endroits auxquels l'utilisation de E_a est interdite. Pour ce faire, nous proposons, à la manière du protocole étudié dans la section 3.1, le protocole suivant :

- Alice calcule $y = E_a(x)$ 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.

Nous l'avons dit, z constitue l'estampille qui atteste l'existence de y à l'endroit s_{AT}. Si l'endroit s_{AT} est différent des endroits auxquels l'utilisation de E_a est interdite alors Alice sera partout en mesure de prouver à quiconque lui en fait la demande que y a été calculé pour nul autre qu'elle et que son contenu n'a pas été altéré par un tripatouilleur. Cette application du marquage spatial des documents électroniques, les règles futures standardisant les conditions de réalisation de la localisation des documents électroniques la mentionneront-elles ?

5.3 Marquage spatio-temporel

De nombreux systèmes bancaires demandent mention de certaines indications précises dans les ordres de paiement écrits qu'ils traitent et certains d'entre eux considèrent qu'un chèque ne peut être payé que s'il comporte la date et le lieu de son tirage. Considérons un message x, par exemple un chèque électronique, et posons $y = f(x)$. Pour prouver à quiconque en fait la demande que $f(x)$ a existé sous sa forme actuelle à une heure donnée à un endroit donné, nous proposons, à la manière du protocole étudié dans la section 4.1, le protocole suivant :

- 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.

Nous l'avons dit, z_{AT} constitue l'estampille qui atteste l'existence de y à l'endroit s_{AT} et z_{AH} constitue l'estampille qui atteste l'existence de z_{AT} à l'heure t_{AH}. Par conséquent, z_{AH} constitue l'estampille qui atteste l'existence de y à l'heure t_{AH} à l'endroit s_{AT}.

6 Problèmes ouverts

Des protocoles horodateurs ont été définis qui sont basés sur les arbres binaires [3] ou les accumulateurs à sens unique [4]. Est-il possible de définir des protocoles topographieurs basés sur les

mêmes principes ? Les protocoles cryptographiques comme ceux décrits par [8] 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 ? Les protocoles considérés dans les sections 2 et 3 recourent à de nombreuses primitives cryptographiques comme les fonctions à sens unique, les fonctions de signature et les générateurs pseudo-aléatoires. Le problème de leur vérification se pose alors dans les mêmes termes que celui de la vérification des protocoles cryptographiques. Les méthodes existantes [2,5] d'analyse de protocoles cryptographiques permettent-elles de le résoudre ?

Remerciements

Nous tenons à remercier les collègues de l'institut de recherche en informatique de Toulouse qui, par les discussions que nous avons eues avec eux, ont contribué à la maturation du travail que nous présentons aujourd'hui.

Références

1. Adams, C., Cain, P., Pinkas, D., Zuccherato, R. : Internet X.509 public key infrastructure time-stamp protocol (TSP). The Internet Engineering Task Force (2001).
2. Armando, A., Basin, D., Bouallagui, M., Chevalier, Y., Compagna, L., Mödersheim, S., Rusinowitch, M., Turuani, M., Viganò, L., Vigneron, L. : The AVISS security protocol analysis tool. Brinksma, E., Larsen, K. (éditeurs) : Computer Aided Verification. Springer-Verlag (2002).
3. Bayer, D., Haber, S., Stornetta, W. : Improving the efficiency and reliability of digital time-stamping. Capocelli, R., De Santis, A., Vaccaro, U. (éditeurs) : Sequences II : Methods in Communication, Security, and Computer Science. Springer-Verlag (1993).
4. Benaloh, J., de Mare, M. : One-way accumulators : a decentralized alternative to digital signatures (extended abstract). Helleseth, T. (éditeur) : Advances in Cryptology – EUROCRYPT '93. Springer-Verlag (1994).
5. Blanchet, B. : An efficient cryptographic protocol verifier based on Prolog rules. 14th Computer Security Foundations Workshop. The Institute of Electrical and Electronics Engineers (2001).
6. Blibech, K. : L'horodatage sécurisé des documents électroniques. Thèse de l'université de Pau et des Pays de l'Adour (2006).
7. Bonnecaze, A., Liardet, P., Gabillon, A., Blibech, K. : Secure time-stamping schemes : a distributed point of view. Annals of Telecommunications **61** (2006).
8. Bozga, L., Ene, C., Lakhnech, Y. : A symbolic decision procedure for cryptographic protocols with time stamps. Journal of Logic and Algebraic Programming **65** (2005).
9. Brassard, G. : Cryptologie contemporaine. Masson (1993).
10. Buldas, A., Laud, P., Lipmaa, H., Villemson, J. : Time-stamping with binary linking schemes. Krawczyk, H. (éditeur) : Advances in Cryptology – CRYPTO '98. Springer-Verlag (1998).
11. Buldas, A., Lipmaa, H., Schoenmakers, B. : Optimally efficient accountable time-stamping. Imai, H., Zheng, Y. (éditeurs) : Public Key Cryptography. Springer-Verlag (2000).
12. Haber, S., Stornetta, W. : How to time-stamp a digital document. Journal of Cryptology **3** (1991).