Université de Montréal

Protocoles cryptographiques pour la Bourse

par
Caroline Peika

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maître ès sciences (M.Sc.)
en informatique

Novembre, 2004

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé:

Protocoles cryptographiques pour la Bourse

présenté par:

Caroline Peika

a été évalué par un jury composé des personnes suivantes:

Alain Tapp,	président-rapporteur
Stefan Wolf,	directeur de recherche
Gilbert Babin,	membre du jury

Mémoire accepté le 19 janvier 2005

Sommaire

Ce mémoire porte sur la modélisation d'un système d'échange d'actions électroniques compte tenu du problème que pose l'exploration de données, problème omniprésent en commerce électronique. L'objectif est de concevoir pour la Bourse un système d'échange d'actions qui respecte certaines règles de sécurité, de telle manière que les parties puissent rester anonymes si elles le désirent. Contrairement à l'argent électronique, certaines restrictions s'appliquent concernant les entités aptes à transiger des actions. Il s'agit, par conséquent, de trouver une méthode permettant d'authentifier les entités impliquées dans une transaction. Si celles-ci souhaitent garder l'anonymat, il faut pouvoir les associer à un groupe – clients du courtier ou négociateurs enregistrés à la Bourse – sans toutefois obtenir leur identité.

Nous analysons les systèmes d'actions électroniques existants et discutons du mode d'échange choisi ainsi que de la sécurité qu'ils offrent. Nous montrons que ces systèmes ne conviennent pas pour modéliser les échanges boursiers. Nous développons un système d'échanges boursiers dans lequel la corrélation des transactions d'une même entité équivaut à la résolution d'un problème difficile. Ce système procure un anonymat inconditionnel aux parties intéressées et peut être adapté pour modéliser d'autres types d'échange d'actions et d'autres types de transactions portant, par exemple, sur d'autres produits financiers.

Mots clés : action électronique, échanges boursiers électroniques anonymes, authentification, anonymat inconditionnel, corrélation de transactions

Abstract

This thesis focuses on the model building of an electronic share system, given the ever present problem of data mining in e-commerce. The aim is to build such a system for the Stock Market – a system that follows specific security rules and protects the privacy of any party wishing to remain anonymous. Unlike for electronic cash, some restrictions apply concerning who can trade e-shares. Hence, a method must be divised to authenticate the parties involved in a transaction before the latter takes place. Should certain parties want to remain anonymous, it must, however, be possible to associate each of them to a group – brokers' clients or traders registered with the Stock Exchange – without obtaining their identity.

We review the existing e-share systems with respect to the type of exchange they use and the security they offer. According to our analysis, those schemes are inadequate to model stock market exchanges. Motivated by this, we design an electronic stock exchange scheme where it is as hard to link together an entity's transactions as it is to solve a difficult problem. Our solution provides unconditional anonymity and can be adapted to other types of markets, securities, and transactions.

Keywords: electronic share, anonymous electronic stock exchange, authentication, unconditional anonymity, linkability

Table des matières

Liste des figures

Liste des tableaux

C'est dans l'effort que l'on trouve la satisfaction et non dans la réussite. Un plein effort est une pleine victoire.

Gandhi

Remerciements

J'aimerais tout d'abord remercier mes parents de m'avoir donné la possibilité de poursuivre des études supérieures. Ils n'ont jamais cessé de m'encourager et d'être pour moi une véritable source d'inspiration.

Je voudrais aussi souligner le rôle de M. Garcia, professeur au département d'économie, dans ce projet. Bien que courte, notre rencontre m'a ouvert des horizons : elle m'a fait découvrir une branche de la cryptographie qui m'intéresse énormément et orienté le choix de mon sujet de mémoire. Je remercie tout particulièrement Vincent Domien, qui m'a éclairée sur certains concepts du domaine financier. Même très occupé, il a bien voulu me donner des explications et répondre à mes questions.

Mille mercis vont aussi à Katerine Martin et Véronique Lefort, sans lesquelles cette expérience aurait été moins agréable et mémorable. Je n'aurais peut-être pas persévéré sans leurs encouragements, leurs conseils, leur appui, leur dynamisme, leur patience, leur réconfort et, surtout, leurs sourires.

Je tiens évidemment à remercier mon directeur, Stefan Wolf, d'avoir pris le temps de m'écouter et d'avoir été disponible aux moments critiques. Ses conseils m'ont été précieux. Enfin, je désire remercier la FES, dont la bourse m'a permis de poursuivre à temps plein la rédaction de ce mémoire.

Introduction

C'est grâce à l'évolution des télécommunications qu'est né le commerce électronique, aujourd'hui en plein essor, et la technologie qui le soutient se développe en conséquence. Par exemple, le consommateur a maintenant le choix entre plusieurs systèmes et modes de paiement électronique ainsi qu'entre un assortiment de produits et de services numériques. La popularité et le développement du commerce électronique sont directement liés à la confiance que celui-ci inspire, principalement la confiance dans la sécurité des protocoles transactionnels et des systèmes de paiement. La possibilité de retracer l'auteur d'une transaction frauduleuse, le cas échéant, contribue aussi à mettre en confiance.

L'échange électronique de titres financiers est une branche du commerce électronique en voie de développement. Comme les règles d'échange varient selon le type de produit financier, presque chaque produit doit avoir des protocoles transactionnels qui lui sont propres.

Il est déjà possible de transiger électroniquement plusieurs produits financiers, mais les actions cotées à la Bourse se transigent uniquement sur le parquet de la Bourse. Le présent projet se propose de créer un système d'échanges boursiers

électroniques. Il tiendra compte des règles d'échange à la Bourse et procurera une sécurité adéquate pouvant inspirer la confiance aux parties intéressées.

La quantité de renseignements personnels généralement exigés pour accéder à de l'information ou pour transiger électroniquement sur un site Internet est discutable. Si elle est accumulée, cette information permet de monter un dossier sur une personne, dossier qui a ses avantages et ses inconvénients. Ainsi, les données privées permettent aux entreprises et aux commerçants d'offrir à la clientèle un service plus personnalisé. Par contre, un tel dossier constitue une atteinte à la vie privée et crée un historique des erreurs commises. Dans le domaine financier, par exemple, tout investisseur peut à l'occasion faire un mauvais choix de placement. Cependant, personne ne veut qu'une erreur passée affecte ses transactions futures et lui vaille mépris ou discrédit. Il existe un moyen d'éviter qu'un mauvais choix ait un effet nuisible sur l'avenir : l'anonymat. Notre projet consiste à créer un système d'échanges boursiers offrant la possibilité de rester anonyme.

Au chapitre 1, nous abordons les thèmes de l'identification et de l'authentification, qui sont omniprésents dans le commerce électronique. Nous définissons ensuite le concept d'anonymat et présentons les divers types d'anonymat. Puis, nous analysons l'impact du désir de rester anonyme sur la nécessité d'identifier les parties à un protocole. Nous poursuivons avec la description du concept d'argent électronique, concept clé dans les transactions électroniques. Après un bref historique des systèmes d'argent électronique, nous examinons en profondeur le système FOLC que nous utiliserons tout au long de ce projet. Des différents systèmes d'argent électronique nous tirons les concepts de base des systèmes d'actions électroniques qui sont étudiés à la fin du chapitre.

Le chapitre 2 présente d'abord les divers modes d'échange possibles d'actions, en insistant sur les échanges boursiers. Les systèmes existants d'échanges d'actions électroniques sont décrits et analysés par la suite. Nous verrons que deux de ces

trois systèmes ne modélisent aucun mode d'échange d'actions et que le troisième ne possède pas un niveau de sécurité approprié.

Comme les trois systèmes analysés au chapitre précédent ne parviennent pas à modéliser les échanges boursiers, le chapitre 3 portera sur la définition du problème de modélisation. Après avoir justifié le besoin de produire pour la Bourse des protocoles d'échanges anonymes, nous décrirons les caractéristiques de tels protocoles en mettant l'accent sur les propriétés de sécurité désirées. La dernière partie du chapitre sera consacrée à la présentation et à l'analyse de trois modèles pouvant offrir une solution. Les deux premiers modèles offrent un anonymat calculatoire et révocable; ils se différencient par leur l'extensibilité. Quant au troisième modèle, notre modèle, il fournit un anonymat inconditionnel.

Chapitre 1

Anonymat: argent et actions électroniques

Le concept d'identité virtuelle est un concept clé dans les communications et les transactions électroniques. Une fois cette identité fournie et authentifiée, le problème de confiance lié aux systèmes électroniques est en partie résolu. Paradoxalement, les consommateurs aimeraient s'abstenir de divulguer cette identité. Ils préféreraient rester anonymes lors de communications ou d'opérations électroniques pour éviter que des organismes gouvernementaux ou privés constituent un dossier sur leurs activités. En particulier, ils souhaitent échanger des biens et des services de manière anonyme et, pour ce faire, un outil leur est offert : l'argent électronique anonyme.

Suite au succès de l'argent électronique, divers produits financiers ont fait leur apparition dans le domaine électronique, en particulier les actions électroniques, qui s'échangent présentement sur Internet dans des transactions pour lesquelles il faut fournir son identité et une authentification. Des progrès restent à accomplir en ce qui a trait à l'anonymat des systèmes d'actions électroniques.

Dans la première section de ce chapitre, l'identité virtuelle sera définie par rapport au concept de personne virtuelle. Le rôle de l'authentification sera ensuite abordé et quelques approches d'authentification seront expliquées. La seconde sec-

tion se propose d'introduire le concept d'anonymat et d'établir un lien avec le concept d'authentification défini à la section précédente. À deux types d'anonymat – inconditionnel et calculatoire, chacun étant révocable ou non – correspondent divers mécanismes d'authentification. La signature en anneau, la signature à l'aveugle et le certificat employé dans un système pseudonymique permettent d'authentifier une clé publique et de rester anonyme. À la troisième section, nous nous pencherons sur les systèmes d'argent électronique. Un système en particulier, le système FOLC, sera décrit en détail en prévision des chapitres suivants. Le système FOLC fournit aux utilisateurs un anonymat révocable. Finalement, la quatrième section portera sur les actions électroniques et le mode d'échange de telles actions. Le thème de l'anonymat sera traité pour chacune des parties impliquées dans l'échange d'actions.

1.1 Identification et Authentification

L'Internet exerce à l'heure actuelle une énorme influence sur les sciences et les techniques et favorise l'intégration des cultures et des économies partout dans le monde. En quelques années, le courrier électronique est devenu un outil de communication au même titre que le téléphone et le télécopieur, et le potentiel du commerce électronique en tant que mécanisme de commerce et d'investissement à l'échelle mondiale ne cesse de croître. L'avantage principal de la communication électronique est qu'elle empêche la discrimination et le stéréotypage basés sur notre identité : nous pouvons enfin être qui nous voulons, qui nous sommes vraiment. Paradoxalement, cet avantage est un inconvénient de taille pour le commerce électronique : commerçants et clients désirent en effet une certaine assurance en ce qui a trait à l'identité des personnes et des institutions avec lesquelles ils font affaires.

1.1.1 Identification

Dans le monde réel, les attributs de la personnalité, notamment le nom patronymique, constituent l'identité d'une personne; ils forment l'ensemble de données nécessaires pour identifier quelqu'un. Nul ne peut s'attribuer soi-même une identité complète qui soit reconnue des autorités publiques. S'identifier exige de fournir des pièces d'identité, une signature manuscrite, une carte de crédit, etc. Diverses institutions, l'État, les banques, les notaires, par exemple, se portent garantes de leur authenticité.

Dans le monde virtuel, pour communiquer ou pour fonctionner, toute personne doit posséder une identité numérique. Pour définir le concept d'identité numérique, il faut tout d'abord définir le concept de personne virtuelle. Une personne virtuelle est le modèle de l'individu établi grâce à la collecte, à l'enregistrement et à l'analyse de données sur cette personne. L'identité numérique est le moyen par lequel des renseignements sont associés à une personne virtuelle. L'identification[1], le processus par lequel il faut fournir une identité numérique, est la fonction principale de l'identité numérique. Et, bien que cette identité doive refléter les propriétés distinctes d'un individu, aucune autorité publique ne garantit sa validité. Un individu peut donc se manifester sous une ou plusieurs identités numériques à la fois.

Traditionnellement, la notion d'identité numérique en cryptographie a été équivalente à la possession d'une clé cryptographique quelconque. Par exemple, dans une infrastructure à clé publique, chaque partie – humain, ordinateur, etc. – possède une paire de clés associées, c'est-à-dire une clé publique et une clé secrète, lui permettant de s'identifier. La clé publique est connue de toutes les parties et la clé secrète, de son détenteur seulement. La confiance en l'identité numérique repose alors sur la provenance de la clé – sur l'entité qui affecte l'identité.

1. La définition de ce concept et du concept d'authentification utilisées dans ce mémoire est celle de Gilles Brassard [4].

Qui distribue les clés? Comment savoir si une clé correspond véritablement à une personne? Qu'un tiers n'utilise pas faussement l'identité? Depuis l'invention de l'identité numérique, l'usurpation d'identité est en hausse. Ce type de délit se produit lorsqu'un tiers utilise les renseignements concernant une personne à l'insu et sans le consentement de celle-ci pour commettre un crime. Une fois que le voleur s'est emparé des renseignements personnels qu'il convoitait, il s'approprie l'identité de la personne. Pour remédier à une telle situation et pour instaurer un plus haut niveau de confiance envers l'identité numérique, plusieurs solutions ont été proposées relatives au choix de l'entité distribuant et gérant les clés et à une procédure d'authentification suivant l'identification.

1.1.2 Authentification

L'authentification complète le processus d'identification; elle permet de prouver une identité déclarée. En commerce électronique, les parties procédant à un échange ou une transaction électronique doivent nécessairement confirmer et valider leur identité.

Définissons Alice et Bob comme étant deux entités procédant à un échange électronique et Ève l'entité malveillante voulant voler l'identité de Bob. Alice et Bob doivent forcément s'identifier et authentifier leur identité respective. Par la suite, ils authentifieront tous les messages qu'ils s'échangeront pour pouvoir détecter si Ève les intercepte ou les remplace. Présentement, la majorité des systèmes d'identification avec authentification considèrent qu'une clé publique correspond à une identité numérique. Pour authentifier cette clé, plusieurs approches ont été développées. Deux d'entres elles sont présentées en détail : la signature numérique et le certificat d'authenticité.

La signature numérique

Une signature numérique est semblable à une signature manuscrite. Pour authentifier un document ou une identité numérique, il s'agit d'y apposer sa signature

numérique. Dans une infrastructure à clé publique, Alice signe un message pour Bob en le cryptant avec sa clé privée. Bob vérifie ensuite la signature à l'aide de la clé publique d'Alice. Toutes les clés publiques valides sont conservées dans un registre public avec le nom, réel ou choisi, de leur propriétaire. L'entité qui gère ce registre reste honnête et impartiale.

Dans cette même infrastructure, en posant M le message qu'Alice veut envoyer à Bob, une signature numérique d'Alice sur M avec sa clé privée s se note

$$sign_s(M)\,.$$

Un message signé est la paire $(M, sign_s(M))$. En le recevant, Bob utilise la clé publique d'Alice pour vérifier la signature. La vérification de la signature avec la clé p se note

$$Ver_p\,(sign_s(M)) = M.$$

Si la signature est acceptée, Bob est assuré de l'intégrité et de la provenance de M. En particulier, pour authentifier son identité, c'est-à-dire sa clé publique, Alice (Bob) envoie à Bob (Alice) un message M fixe – l'identité déclarée à cet instant.

Plusieurs variantes de la signature numérique existent. Pour le présent projet, les plus pertinentes sont la signature en anneau (*ring signature*) et la signature à l'aveugle juste (*fair blind signature*). Elles seront présentées dans la prochaine section, qui porte sur l'anonymat.

Le certificat numérique

Un certificat numérique est une solution de rechange au registre de clés publiques, car il peut parfois être fastidieux de gérer et d'utiliser un tel registre. Un certificat est une déclaration signée qui lie une clé publique à l'identité (numérique ou réelle) de son propriétaire. Authentifier une clé publique consiste à fournir un certificat. La validité du certificat est directement liée à la confiance accordée à l'autorité signant les déclarations. Cette entité détermine le profil du certificat,

lequel comprend généralement la clé publique, l'identité de son propriétaire et la date d'expiration du certificat. On note

$$Cert_{CA}(p, X)$$

un certificat signé par l'autorité de certification (CA) pour la clé publique p et l'identité X. L'autorité gère aussi une liste publique des certificats révoqués, c'est-à-dire non valides ou volés. Cette liste et la date d'expiration des certificats sont le sujet de nombreux débats portant sur l'amélioration de l'efficacité d'un système de certification; la validité des certificats repose sur ces deux points.

Le certificat peut être utilisé en symbiose avec la signature numérique. Alice fournit à Bob le certificat correspondant à sa clé publique. Bob vérifie que le certificat n'est pas expiré et que la signature de l'autorité de certification est valide. Par ailleurs, Alice fournit une signature numérique à Bob pour authentifier sa clé. De cette manière, Bob est certain que la personne qui lui a fourni le certificat est bien celle avec qui il communique.

Pour exister dans le monde virtuel, il est nécessaire d'avoir une identité numérique. Comme une personne peut elle-même choisir et créer sa propre identité numérique, des mécanismes d'authentification ont été pensés pour fournir une protection et une assurance lors de transactions ou d'échanges électroniques. Les signatures numériques et les certificats associent une clé publique à une identité et fournissent un moyen d'authentifier cette clé. L'usage de protocoles d'identification et d'authentification semble s'accroître à l'excès. Par conséquent, les utilisateurs souhaitent de plus en plus protéger leur identité et pouvoir rester anonyme sans s'interdire l'accès aux sites ou aux serveurs qui demandent une identification et une authentification.

1.2 Anonymat

L'énorme popularité d'Internet révèle à quel point la nouvelle technologie suscite l'intérêt. De plus en plus de biens et de services personnalisés sont offerts sur Internet pour attirer davantage les utilisateurs. Ces derniers doivent souvent « s'identifier » pour accéder aux sites ou aux réseaux en fournissant un grand nombre de renseignements personnels. Cette identification n'est cependant pas nécessairement dans l'intérêt de l'utilisateur. En effet, bien que la vitesse, l'efficacité et la sécurité soient les motifs invoqués pour justifier l'identification, celle-ci sert majoritairement au marketing par secteurs cibles et à la création de dossiers. Pour se protéger contre l'accès à leur vie privée, certains utilisateurs préfèrent ne fournir aucune information privée et rester anonymes.

1.2.1 Définition

En cryptographie, une entité, que nous appelons Alice, veut transmettre un message M à une seconde entité, Bob. Dire qu'Alice souhaite rester anonyme c'est dire qu'elle désire que son identité ne soit pas liée au message transmis à Bob, notamment à la clé utilisée si le message est crypté. En recevant M, Bob ne doit pas connaître avec certitude l'identité de l'expéditeur. De son côté, Bob, le récepteur du message, peut lui aussi vouloir demeurer anonyme. Dans ce cas, Alice transmet M de façon à ce que seul Bob puisse le recevoir, sans toutefois savoir que le receveur est effectivement Bob. Si plusieurs messages sont transmis et si Alice et Bob veulent rester anonymes, l'analyse des messages et de leur transmission ne doit pas révéler d'information sur les identités des deux parties. Dans le présent document, les canaux de communication sont considérés comme étant anonymes, l'anonymat ne pouvant donc pas être compromis par le canal en soi.

Être anonyme signifie ne pas être distinguable à l'intérieur d'un groupe particulier. L'expéditeur d'un message, par exemple, est anonyme parmi l'ensemble des expéditeurs possibles et le receveur d'un message est anonyme parmi l'ensemble des receveurs possibles.

1.2.2 Types d'anonymat

Anonymat inconditionnel

Dans une infrastructure à clé publique, une entité est inconditionnellement anonyme si, selon la théorie de l'information, il n'est pas possible d'associer avec parfaite certitude son identité (numérique ou réelle) à sa clé publique. Plus exactement, la meilleure stratégie pour trouver l'identité est de la deviner, quels que soient le nombre de messages transmis et la puissance de calcul utilisée. L'anonymat ne dépend d'aucune hypothèse cryptographique autre que celle de l'existence d'une source générant des nombres aléatoires. Un parallèle peut être établi entre la sécurité parfaite d'un cryptage et l'anonymat parfait. Dans le premier cas, le message est statistiquement indépendant du cryptage alors que dans le deuxième, la clé publique est statistiquement indépendante de l'identité.

Dans certaines situations, il est indispensable de fournir un indice relatif à l'identité sans toutefois devoir compromettre l'anonymat, c'est-à-dire authentifier la clé publique utilisée. Rivest, Shamir et Trauman [24] proposent un moyen de prouver l'appartenance à un groupe tout en restant inconditionnellement anonyme. Dans ce cas, accepter de communiquer ou de transiger avec l'entité anonyme dépend de la confiance accordée aux entités constituant le groupe. Rivest *et al.* formalisent une nouvelle signature de groupe (*group signature*) : la signature en anneau (*ring signature*). Puisque cette signature sera mentionnée à maintes reprises dans les prochains chapitres, il est intéressant d'en décrire sommairement les étapes (certains détails seront omis).

La signature en anneau

Le signataire, nommé P_l, fait partie d'un ensemble $\mathcal{P}$, $\mathcal{P} = \{P_1, \ldots, P_l, \ldots, P_t\}$. Tout $P_i \in \mathcal{P}$ possède une clé publique p_i certifiée et associée à une clé privée s_i dans une infrastructure à clé publique.

En premier, le signataire choisit un sous-ensemble $\mathcal{P}'$ de $\mathcal{P}$ de signataires possibles dont il fait inévitablement partie. Posons $\mathcal{P}' = \{P_1, \ldots, P_r\}$ les membres de la signature et $p_1, \ldots, p_r$ leur clé publique respective; on sait que $\mathcal{P}' \subseteq \mathcal{P}$. Ensuite, le signataire fournit une fonction de hachage à collisions difficiles, h, une permutation à sens unique avec brèche secrète g_i propre à chaque membre P_i et une fonction $C_{k,v}(y_1, \ldots, y_r)$ qui prend en entrée une clé k, une valeur d'initialisation v et des valeurs arbitraires $y_1, \ldots, y_r$ et qui a des propriétés précises, à savoir :

1. la fonction C permute chaque entrée,
2. si k, v et $y_1, \ldots, y_r$ sauf y_i sont connus, résoudre $C_{k,v}(y_1, \ldots, y_r) = z$ pour y_i est efficace,
3. si k, v et z sont connus, il est infaisable de résoudre l'équation $C_{k,v}(g_1(x_1), \ldots, g_r(x_r)) = z$ pour toutes les entrées $y_1, \ldots, y_r$ sans connaître les brèches secrètes des fonctions de permutation $g_1, \ldots, g_r$.

De prime abord, on pense à utiliser le OU exclusif comme fonction C. Cependant, le OU exclusif ne satisfait pas la troisième propriété essentielle. En effet, pour un r assez grand et tout choix de fonctions de permutation avec brèche secrète $g_1, \ldots, g_r$, il est possible de trouver une solution $x_1, \ldots, x_r$ sans inverser de g_i. L'attaque précise est décrite dans [24]. Un choix valable pour la fonction C serait un amalgame de OU exclusif et de cryptage symétrique, noté E_k :

$$C_{k,v}(y_1, \ldots, y_r) = E_k(y_r \oplus E_k(y_{r-1} \oplus (E_k(y_{r-2} \oplus E_k(\ldots \oplus (E_k(y_1 \oplus v)\ldots))))$$

La génération d'une signature sur un message m se déroule comme suit :

a. P_l calcule la clé symétrique k, $k = h(m)$.

b. Il choisit ensuite, de façon aléatoire et uniforme, la valeur d'initialisation v.

c. Pour tous les autres membres, P_l choisit de façon aléatoire et indépendante une valeur x_i. Il calcule alors $y_i = g_i(x_i)$ pour $1 \leq i \leq r$, $i \neq l$.

d. Il résout $C_{k,v}(y_1, \ldots, y_r) = v$ par rapport à y_l.

e. Il utilise sa connaissance de la brèche secrète pour inverser g_l et trouver x_l : $x_l = g_l^{-1}(y_l)$. La signature produite est : $(m, (P_1, \ldots, P_r\,;\, v\,;\, x_1, \ldots, x_r))$.

L'entité qui doit vérifier la signature $(m, (P_1, \ldots, P_r\,;\, v\,;\, x_1, \ldots, x_r))$ accomplit les étapes suivantes :

a. Elle trouve les y_i à l'aide des x_i reçus : $y_i = g_i(x_i)$ pour $1 \leq i \leq r$.
b. Elle calcule la clé k à partir de m : $k = h(m)$.
c. Elle vérifie que l'égalité suivante tient : $C_{k,v}(y_1, \ldots, y_r) = v$. Dans l'affirmative, la signature reçue est valide.

Étant donné un groupe de r signataires possibles, il y a 1 possibilité sur r de trouver l'identité du véritable signataire. Malgré les hypothèses cryptographiques utilisées, comme l'existence d'une fonction avec brèche secrète, l'anonymat fourni par cette signature est inconditionnel; un adversaire avec des ressources illimitées et une infinité de messages signés choisis n'est pas avantagé dans la recherche de l'identité. Cependant, il est calculatoirement difficile de générer une signature valide si l'on n'appartient pas au groupe.

Anonymat calculatoire

L'anonymat dit calculatoire est basé sur une ou plusieurs hypothèses cryptographiques nommées hypothèses calculatoires. Elles portent sur la difficulté (démontrée ou non) de résoudre certains problèmes étant donné une puissance de calcul limitée, c'est-à-dire étant donné la puissance de calcul maximale existante.

Si l'anonymat d'une entité est basé sur une telle hypothèse d'insolubilité, trouver l'identité de l'entité se réduit à résoudre un problème considéré comme difficile compte tenu la puissance de calcul maximale existante. L'identité est complètement dissimulée tant que l'hypothèse, bien établie ou non, tient. Les problèmes difficiles et les hypothèses les plus pertinents à ce projet sont énumérés dans les tableaux 1.1 et 1.2 respectivement.

Problème	Description
Logarithme discret	Étant donné un nombre premier p, un générateur α de $\mathbb{Z}_p^*$ et un élément $\beta \in \mathbb{Z}_p^*$, trouver l'entier x, $0 \leq x \leq p-2$, tel que $\alpha^x \equiv \beta \pmod{p}$.
Logarithme discret généralisé	Étant donné un groupe cyclique fini $\mathcal{G}$ d'ordre n, un générateur α de $\mathcal{G}$ et un élément $\beta \in \mathcal{G}$, trouver un entier x, $0 \leq x \leq n-1$, tel que $\alpha^x = \beta$.
Diffie-Hellman	Étant donné un nombre premier p, un générateur α de $\mathbb{Z}_p^*$ et les deux éléments $\alpha^c \bmod p$ et $\alpha^d \bmod p$, trouver $\alpha^{cd} \bmod p$.
Diffie-Hellman généralisé	Étant donné un groupe cyclique fini $\mathcal{G}$, un générateur α de $\mathcal{G}$ et les éléments a^c et a^d, trouver a^{cd}.
Diffie-Hellman version décision	Étant donné un groupe $\mathcal{G}$, un générateur g de $\mathcal{G}$ et trois éléments a, b, c de $\mathcal{G}$, décider s'il existe deux entiers x et y tels que $a = g^x$, $b = g^y$ et $c = g^{xy}$.

TAB. 1.1 – *Problèmes jugés difficiles*

Pour fournir une assurance tout en restant anonyme, il est possible de créer une signature en anneau où le signataire reste anonyme tant qu'une hypothèse cryptographique tient et, contrairement à la signature en anneau dont l'anonymat est inconditionnel, il peut aussi prouver qu'il a bel et bien signé lui-même le message. Il choisit de façon pseudo-aléatoire, plutôt qu'aléatoire, les valeurs x_i des membres et, pour prouver qu'il est l'auteur de la signature, il peut fournir la valeur de départ qu'il a utilisée pour générer les x_i. Prouver l'appartenance au groupe revient à fournir une signature en anneau; prouver que l'on est le signataire revient à fournir la valeur de départ. Par ailleurs, trouver l'identité du signataire exige la résolution d'un problème considéré comme difficile.

Hypothèse	Description
Logarithme Discret	Il y a des groupes pour lesquels il n'existe pas d'algorithme efficace permettant de calculer un logarithme discret.
Diffie-Hellman	Il y a des groupes pour lesquels il n'existe pas d'algorithme efficace permettant de résoudre le problème Diffe-Hellman.
Diffie-Hellman version décision	Il y a des groupes pour lesquels il n'existe pas d'algorithme efficace permettant de résoudre le problème Diffe-Hellman version décision.

TAB. 1.2 – *Hypothèses calculatoires*

1.2.3 Anonymat révocable

L'anonymat inconditionnel et l'anonymat calculatoire peuvent tous deux être révocables. L'anonymat défini comme révocable est limité, c'est-à-dire il existe un moyen efficace de trouver l'identité de l'entité anonyme. Généralement, un tiers de confiance ou une entité désignée possède une information secrète qui permet d'exposer l'identité soit en vérifiant dans un registre, soit en effectuant des calculs.

L'entité qui utilise des méthodes procurant un anonymat révocable telles que la signature à l'aveugle juste et le CAPK fournit une garantie – une authentification en quelque sorte – de son identité tout en restant anonyme.

a. La signature à l'aveugle juste

La signature à l'aveugle, créée par Chaum expressément pour modéliser un système de paiment électronique [5], permet à Alice d'obtenir une signature de Bob sur un message sans que Bob n'obtienne d'information sur le message. La signature à l'aveugle juste (*fair blind signature*) [29] est une variante de cette signature. Elle offre une garantie de l'identité de l'entité qui a demandé et reçu la signature; on peut efficacement retracer son identité. Un tiers de confiance peut, sur demande, faire correspondre un message non signé au même message signé et même établir le lien avec l'identité de la personne qui a envoyé le message (et obtenu la signature).

Les protocoles de signature et de retracement sont décrits dans [29].

Supposons qu'Alice est l'entité désirant communiquer (transiger, échanger, etc.) anonymement avec Bob. Pour fournir un indice quant à son identité, Alice envoie à Bob un message portant une signature à l'aveugle juste d'une autorité quelconque. Si Bob veut obtenir l'identité d'Alice, il remet le message signé qu'il a reçu d'Alice à l'autorité signataire. Le tiers de confiance peut ensuite trouver l'identité d'Alice.

b. Le CAPK

Un CAPK, l'acronyme venant de *Certified Anonymous Public Key*, est une clé publique anonyme qui n'est pas publiquement liée à une identité et qui est certifiée par une autorité de certification. L'anonymat procuré par la clé peut être révoqué par un tiers de confiance uniquement. Lors de l'acquisition du certificat, l'entité fournit une information qui sera modifiée et inclue dans le certificat et qui permettra à un tiers de confiance de révoquer l'anonymat s'il y a lieu. Noté $Cert_{CA}(p, X)$, le certificat authentifie la clé anonyme p par rapport à la valeur X. Cette valeur n'est pas l'identité numérique du propriétaire de la clé p, mais une information qui n'est utile qu'au tiers de confiance, lui permettant de retracer l'identité du propriétaire.

1.3 Argent électronique

Que ce soit pour un échange d'information ou pour une opération financière, le besoin de trouver des techniques pour assurer l'anonymat augmente au même rythme que le besoin d'inventer des techniques pour garantir l'identité d'une personne. En particulier, l'argent électronique a été créé dans le but de fournir le même niveau d'anonymat que le papier-monnaie mais, pour des raisons de sécurité, on cherche à diminuer cet anonymat.

1.3.1 Glossaire

Plusieurs termes clés sont utilisés dans le domaine du commerce électronique. Dans les paragraphes suivants, les concepts propres aux systèmes d'argent électronique sont définis afin d'éliminer toute ambiguïté.

L'argent électronique (*e-cash*) est un mode de paiement dont la valeur monétaire est représentée sous forme numérique. La banque émet des pièces électroniques (*e-coins*) qui correspondent à une somme d'argent précise. Pour alléger le texte, le terme pièce signifiera pièce électronique.

Un système d'argent électronique comprend trois acteurs essentiels soit la banque, le client – le propriétaire d'une pièce – et le commerçant. Comme cela a été mentionné précédemment, la banque crée les pièces. Le client et le commerçant possèdent chacun un compte bancaire d'où ils peuvent respectivement retirer et déposer de l'argent électronique. Une fois les pièces retirées, le client les dépense chez le commerçant. Inévitablement, le système comporte un protocole de retrait, un protocole de paiement et un protocole de dépôt.

On dit d'un système d'argent électronique qu'il est autonome (*off-line*) si les entités administratives, comme la banque ou un tiers de confiance, ne jouent aucun rôle dans le protocole de paiement. Un système d'argent électronique anonyme est juste (*fair*) si l'identité du client est dissimulée dans la pièce retirée à la banque

et seuls un ou plusieurs tiers de confiance, incluant généralement un juge, peuvent facilement la retrouver. Le système d'argent électronique peut avoir comme propriété que les pièces électroniques ou les paiements électroniques ne peuvent être reliés entre eux (*unlinkable*).

1.3.2 Historique

En premier lieu, l'argent électronique a été créé dans le but d'automatiser les paiements et de fournir le même niveau d'anonymat aux propriétaires que le papier monnaie. Puis, avec l'effervescence des transactions électroniques, les méthodes de marketing par secteur ont été développées pour analyser les intérêts des consommateurs. Par conséquent, les besoins des utilisateurs d'argent électronique ont changé. À ce jour, les utilisateurs veulent non seulement être anonymes lors de leurs achats, mais souhaitent que leurs différents achats ne puissent être reliés entre eux.

En 1982, David Chaum [5] décrit le premier système de paiement électronique où les pièces d'un même utilisateur ne peuvent être reliées entre elles; l'anonymat est inconditionnel. Cependant, les pièces peuvent être facilement copiée et utilisée en double. Plus précisément, la création de pièces est possible sans la coopération de la banque. La correction de cette lacune figure dans l'article de Chaum, Fiat et Naor [6]. Si une pièce est doublement dépensée, la banque peut retracer le compte d'où elle a été retirée et prouver que la pièce a été utilisée à deux occasions. Sinon, l'identité de l'utilisateur est inconditionnellement cachée. Dans ce même article, une nouveauté est introduite : la banque n'intervient plus pendant le paiement. Elle demeure autonome (*off-line*). L'analyse de ce nouveau système soulève néanmoins le problème des crimes parfaits [28]. L'anonymat de l'utilisateur est tel que la fraude, les ventes illégales, l'extorsion et le blanchiment d'argent peuvent avoir lieu sans que les criminels puissent être retracés. On en vient donc à la conclusion qu'il faut limiter l'anonymat de l'utilisateur d'argent électronique. Les systèmes d'argent électronique justes font alors leur apparition. Ils équilibrent le besoin d'anonymat du client et le besoin de protéger la banque et ses clients honnêtes

contre la mauvaise utilisation de pièces. L'identité du client est dissimulée dans la pièce et ne peut être retrouvée qu'avec l'aide d'un tiers de confiance seulement; sinon, l'utilisateur reste anonyme.

Le système qui sera utilisé dans ce projet a pour nom *fair off-line e-cash*, FOLC, et se base sur [12], [13], [11], [31] et [14]. L'existence de ce système a été prouvée dans [12] et [14].

1.3.3 FOLC

Le système d'argent électronique FOLC diffère des autres systèmes par le fait que l'anonymat du client de la banque est contrôlé. Un tiers de confiance peut révoquer l'anonymat dudit client à certaines conditions seulement, conditions dépendant des réglementations sur le commerce électronique. Les acteurs dans ce système sont : la banque « B », un client de la banque « U », un commerçant « C », un tiers de confiance, « T » et une autorité de certification « CA ». Les cinq protocoles suivants définissent le système FOLC.

Protocole de retrait : U obtient une pièce de B qui débite le compte de U du montant correspondant.

Protocole de paiement : U paie C en utilisant la pièce qu'il a retirée.

Protocole de dépôt : C remet à B la pièce reçue lors du paiement et B crédite C du montant correspondant.

Le tiers de confiance, propre aux systèmes justes, intervient dans les deux autres protocoles : le protocole de retracement du propriétaire qui permet de trouver l'origine de pièces suspectes dans des situations telles que le blanchiment d'argent, et le protocole de retracement de pièce, qui permet de trouver la destination de pièces suspectes.

Protocole de retracement du propriétaire : B donne un aperçu du protocole de dépôt à T qui lui remet de l'information pouvant identifier le client ayant retiré la pièce. Par la suite, B fait le lien entre la pièce et le client.

Protocole de retracement de la pièce : T, qui a reçu de B un aperçu du protocole de retrait, communique à B une information que lui seul peut obtenir. Cette information permet d'apparier une pièce retirée à une pièce déposée.

Description technique des protocoles de FOLC

La banque utilise un canal authentifié pour communiquer avec ses clients tandis que ces derniers utilisent un canal anonyme pour communiquer avec les commerçants.

Procédure d'initialisation de la banque (accomplie une seule fois)
La banque choisit un groupe $\mathbb{Z}_p^*$ et un sous-groupe $\mathcal{G}_q$ de $\mathbb{Z}_p^*$ tels que $|p-1| = \delta + k$ pour une constante δ et $p = \gamma q + 1$ pour un entier γ (pour une description plus détaillée, voir [13]). Puis, elle choisit dans $\mathcal{G}_q$ cinq générateurs, g, g_1, g_2, g_3, g_4, ainsi qu'une clé secrète aléatoire X_B. La clé X_B correspond à la dénomination des pièces créées. Il est nécessaire d'avoir une clé différente pour chaque dénomination mais nous supposons, dans le cas présent, qu'il n'y en a qu'une seule. Finalement, elle choisit des fonctions de hachage $\mathcal{H}$, $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2, \ldots$ provenant d'une famille de fonctions de hachage à collisions difficiles. Elle rend les valeurs suivantes disponibles : p, q, g, g_1, g_2, g_3, g_4, $\mathcal{H}$, $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2, \ldots$, et ses clés publiques : $h = g^{X_B}$, $h_1 = g_1^{X_B}$, $h_2 = g_2^{X_B}$, $h_3 = g_3^{X_B}$.

Procédure d'initialisation du tiers de confiance (accomplie une seule fois)
Le tiers de confiance choisit une clé privée $x_T \in \mathcal{G}_q$ et met à la disposition de tous ses deux clés publiques : $f_2 = g_2^{x_T}$ et $f_3 = g_3^{x_T}$.

Procédure d'initialisation du client (ouverture d'un compte bancaire)
Le client choisit une valeur aléatoire $u_1 \in \mathcal{G}_q$, qu'il garde secrète, et fournit $I = g_1^{u_1}$ modulo p à la banque, en guise d'identité. Ensuite, il prouve à la banque qu'il connaît u_1.

Retrait

Le protocole de retrait produit une signature à l'aveugle restrictive (*restrictive blind signature*) sur l'identité du client, sur I, et sur une information propre à la pièce produite. La signature permet de retracer la pièce et crypte l'identité du client. La pièce produite est $A = g_1^{u_1} g_2^s g_3$. Le protocole de retrait est décrit dans le tableau 1.3. Une preuve à divulgation nulle de l'équivalence de logarithmes, notée EqLog, est utilisée pour vérifier si la construction de la pièce est adéquate. Le protocole $\mathsf{EqLog}[(A,a), G_1, (B,b), G_2]$ permet de prouver que $A = a^x G_1^v$ et $B = b^x G_2^w$ c'est-à-dire que $\log_a A = \log_b B$. E_1 et E_2 sont des cryptages ElGamal de g_2^s.

U (client)		**B (banque)**
$m,\ s,\ t \in_R \mathcal{G}_q$ $I' = (g_1^{u_1})^{s^{-1}} (g_3)^{s^{-1}} (g_4)^t$ $E_1 = g_2^s f_3^m,\ E_2 = g_3^m$ $V_1 = \mathsf{EqLog}[(E_1,\ f_3),\ g_2,\ (E_2,\ g_3),\ nil]$ $V_2 = \mathsf{EqLog}[(g_3,\ I'),\ (g_1,\ g_4),\ (E_1,\ g_2),$ $f_3,\ (I,\ I'),\ (g_3,\ g_4)]$		
	$\xrightarrow{I', E_1, E_2, V_1, V_2}$	
		$E_2 \neq 1$? Vérifier V_1,V_2 $w \in_R \mathcal{G}_q$ $a' = g^w$ $b' = (I' g_2)^w$ $b'' = g_2^w$
	$\xleftarrow{a', b', b''}$	
$A = g_1^{u_1} g_2^s g_3$ $z = h_1^{u_1} h_2^s h_3$ $x_1,\ x_2,\ u,\ v \in_R \mathcal{G}_q$ $B = g_1^{x_1} g_2^{x_2}$ $a = (a')^u g^v$ $b = (b'(b'')^{t^{-1}})^{su} A^v$ $c = \mathcal{H}(A, B, z, a, b)$ $c' = \frac{c}{u}$		
	$\xrightarrow{c'}$	
	$\xleftarrow{r'}$	$r' = c' X_B + w$
$r \equiv r'u + v \pmod q$ Vérifier $g^r = h^c a$? et $A^r = z^c b$?		

TAB. 1.3 – *Protocole de retrait du système FOLC*

Paiement

Le client transmet au commerçant de l'information qui permettra d'identifier le client si ce dernier utilise une pièce en double. Formellement, le client produit une signature sur la pièce retirée A qu'il communique au commerçant en plus de la valeur $A_2 = f_2^s$. Il prouve qu'ensemble, ces deux valeurs forment un cryptage ElGamal de I. Le protocole de paiement se trouve dans le tableau 1.4.

U (client)		**C (commerçant)**
$A_1 = g_1^{u_1} g_2^s$ $A_2 = f_2^s$ $E_1 = g_2^s f_3^m$, $E_2 = g_3^m$ $V_3 = \mathsf{EqLog}[(A_2, g_2), g_1, (A_2, f_2), nil]$	$\xrightarrow{A_1, A_2, B, (z,a,b,r)}$	
		$A_1 \neq 1$? $A_1 g_3 = A$ $sign_C(A, B) = (z, a, b, r)$? Vérifier V_3

TAB. 1.4 – *Protocole de paiement du système FOLC*

Dépôt

Le commerçant fournit à la banque une transcription du protocole de paiement. La banque vérifie alors la validité du protocole.

Retracement du propriétaire

La banque transmet la pièce déposée au tiers de confiance. Ce dernier utilise sa clé privée pour décrypter le cryptage ElGamal de A_1 et de A_2; il obtient I et le communique à la banque.

Retracement de la pièce

La banque transmet la transcription du protocole de retrait au tiers de confiance qui décrypte le cryptage ElGamal de E_1 et de E_2 pour obtenir la valeur g_2^s. La banque trouve la pièce associée $A = I\, g_2^s g_3$.

Propriétés

Le système FOLC garantit les propriétés suivantes :

P1 : Le client légitime est anonyme.

P2 : Sous présentation d'une justification, l'anonymat peut être révoqué.

P3 : La double utilisation d'une pièce révèle l'identité de son propriétaire.

P4 : Les protocoles de retracement et les autres protocoles sont efficaces.

P5 : Les pièces créées par la banque sont infalsifiables.

P6 : Seule la banque peut créer les pièces.

P7 : Il ne peut y avoir collusion, par exemple, entre la banque, le tiers de confiance et le commerçant pour connaître l'identité du client.

P8 : L'identité du client n'est pas compromise par les pièces qu'il a retirées et dépensées.

Sécurité

La sécurité des protocoles du système FOLC est basée sur la sécurité du système d'argent électronique de Brands [3], ainsi que sur les propriétés de la preuve à divulgation nulle d'équivalence de logarithmes. Plus précisément, l'anonymat du client, correspondant aux propriétés P1, P7 et P8, est fondé sur la sécurité sémantique du cryptage ElGamal, c'est-à-dire que trouver l'identité équivaut à démentir l'hypothèse Diffie-Hellman version décision et vice versa. Par ailleurs, la révocation de l'anonymat, correspondant aux propriétés P2, P3 et P4, se fonde sur la propriété d'exactitude (*correctness*) de la preuve à divulgation nulle de l'équivalence de logarithmes ainsi que sur l'hypothèse Logarithme discret. Révoquer l'anonymat équivaut à trouver un logarithme discret. Enfin, la sécurité pour le commerçant et la banque, soit les propriétés P5 et P6, est basée sur les propriétés de la signature à l'aveugle restrictive et est équivalente à la sécurité du cryptage El Gamal. La signature à l'aveugle utilisée dans les protocoles FOLC est considérée comme étant restrictive, mais la preuve de ceci n'en a pas encore été fournie.

1.4 Actions électroniques

Tout comme le commerce électronique, les transactions bancaires sur Internet connaissent une grande popularité. Le client de la banque est libre de consulter son compte bancaire, de payer ses factures, de virer des fonds, ..., au moment qu'il juge opportun; sur Internet, la banque est ouverte 24 heures sur 24. La réussite de la banque électronique motive les institutions financières à favoriser la vente et l'achat de leurs produits de manière électronique. Déjà, les consommateurs peuvent vendre et acheter certains produits financiers sur Internet. En particulier, ils ont accès au marché Nasdaq, un marché hors cote, où il est possible d'échanger des actions. Cependant, il n'est toujours pas possible d'échanger des actions à la Bourse sur Internet, anonymement ou non.

1.4.1 Définition

Une action électronique (*e-share*) est un titre financier qui peut être transigé électroniquement, par exemple, sur Internet. Une action électronique possède les mêmes caractéristiques que son pendent non électronique : elle peut générer des dividendes, elle peut être vendue ou achetée n'importe quand, les revenus en dividendes ou provenant de la vente sont imposables et elle donne généralement un droit de vote à son propriétaire. Une action électronique possède la propriété d'être infalsifiable. Seule une entité désignée émet les actions; nul ne peut les copier ou en créer.

Un investisseur, soit un particulier ou un organisme ayant de larges sommes à investir, achète ou vend une action de l'une des façons suivantes : en échangeant son action directement avec un autre investisseur (ce qui est très rare), en l'échangeant sur un marché hors cote (certains titres seulement) ou en transigeant à la Bourse (la majorité des cas). Ces trois modes d'échange seront expliqués au prochain chapitre. Quel que soit le moyen choisi pour échanger une action électronique, celle-ci ne doit pas pouvoir faire l'objet d'une double vente : une fois que le propriétaire l'a vendue, l'action ne lui appartient plus; il ne peut la vendre en double (*double-spent*).

1.4.2 Système d'actions électroniques

Un système d'actions électroniques comporte au moins les parties suivantes : une entreprise, un serveur et des investisseurs. La compagnie décide d'émettre ou de retirer des actions électroniques et avise le serveur de sa décision. Ce dernier exécute la décision tout en gérant l'inventaire d'actions électroniques de l'entreprise. Les investisseurs achètent et vendent ces actions de manière électronique.

Pour fonctionner, un système d'actions électroniques nécessite un système d'argent électronique et comporte donc, en plus de protocoles d'achat et de vente d'action, des protocoles propres au système d'argent électronique, c'est-à-dire des protocoles de retrait, de paiement et de dépôt. Il est important de souligner que les protocoles d'achat et de vente d'actions dépendent du mode d'échange choisi.

On dit qu'un système d'actions électroniques est autonome (*off-line*) quand le serveur et toute autre entité administrative sont absents lors de l'échange d'une action et que le système d'argent électronique utilisé est lui aussi autonome.

1.4.3 Anonymat

On trouve aussi le désir d'anonymat chez les parties impliquées dans l'échange d'actions. Quel que soit le mode d'échange employé, les investisseurs ne veulent pas révéler leur identité pour éviter que quiconque puisse analyser leurs activités financières. En particulier, les autres investisseurs peuvent profiter de la recherche d'information et de l'analyse qui a menée aux transactions. Les investisseurs veulent aussi se protéger contre la création d'un dossier par crainte que leurs activités passées nuisent à leurs activités présentes.

Un système d'actions électroniques a la propriété d'être anonyme si les protocoles de vente et d'achat ne divulguent aucune information sur l'identité des entités impliquées. Un système d'actions électroniques anonyme est juste (*fair*) lorsque l'identité du propriétaire de l'action peut être retrouvée efficacement par une tierce personne désignée. Le système d'actions électroniques peut aussi avoir comme propriété qu'aucun lien ne peut être établi entre les échanges (*unlinkable*).

Chapitre 2

Systèmes d'actions électroniques existants

De nos jours, il existe un vaste éventail de produits et de marchés financiers. Les investisseurs peuvent investir dans un produit comportant le niveau de risque qu'ils sont prêts à assumer. S'ils sont en mesure de prendre un certain risque, ils choisiront, par exemple, de transiger des actions.

Les modes de transaction de produits d'investissement font de plus en plus appel à la technologie, incluant, depuis peu, les échange d'actions. Plusieurs systèmes d'échanges d'actions électroniques ont déjà été créés; ils garantissent tous qu'aucun lien ne peut être établi entre une transaction et l'identité de l'investisseur. Bien que ces systèmes se disent conformes, ils ne conviennent pas tout à fait aux modes d'échange d'actions réels.

La première section de ce chapitre traite des modes d'échange d'actions existants. Un système d'actions électroniques doit modéliser un de ces modes afin de correspondre aux marchés réels. La deuxième section présente les systèmes d'échange d'actions déjà proposés : acteurs, protocoles et analyse des différents systèmes. Un lien sera établi entre les marchés existants et ce qui a été proposé. La dernière section reliera tous ces éléments d'analyse entre eux et donnera un aperçu de ce qu'il reste à accomplir.

2.1 Modes d'échange d'actions électroniques

Il existe plusieurs marchés où les actions peuvent être transigées et chaque marché possède son propre mode d'échange. Pour les systèmes d'actions électroniques anonymes qui seront présentés plus loin, les auteurs disent modéliser un mode d'échange d'actions. Pour bien comprendre le fonctionnement de ces systèmes et les lacunes qu'ils comportent, il faut d'abord saisir quels sont les modes d'échange d'actions possibles.

1- Marché institutionnel ou quatrième marché

Le marché institutionnel est un mode d'échange entre deux investisseurs qui est très rarement utilisé. Sur les marchés hors cote et boursier, il y a un maximum d'actions d'une même entreprise qui peut être transigé en une journée et d'un seul coup. Pour contourner cette limite, le propriétaire d'un grand nombre d'actions qui souhaite s'en défaire en une seule opération de vente peut y parvenir s'il trouve lui-même un acheteur potentiel. Dans ce cas, les deux parties concluent une entente pour que les actions changent de propriétaire, entente ayant peu d'influence sur le prix des actions.

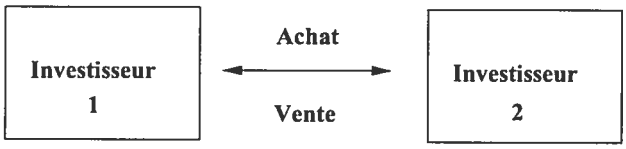
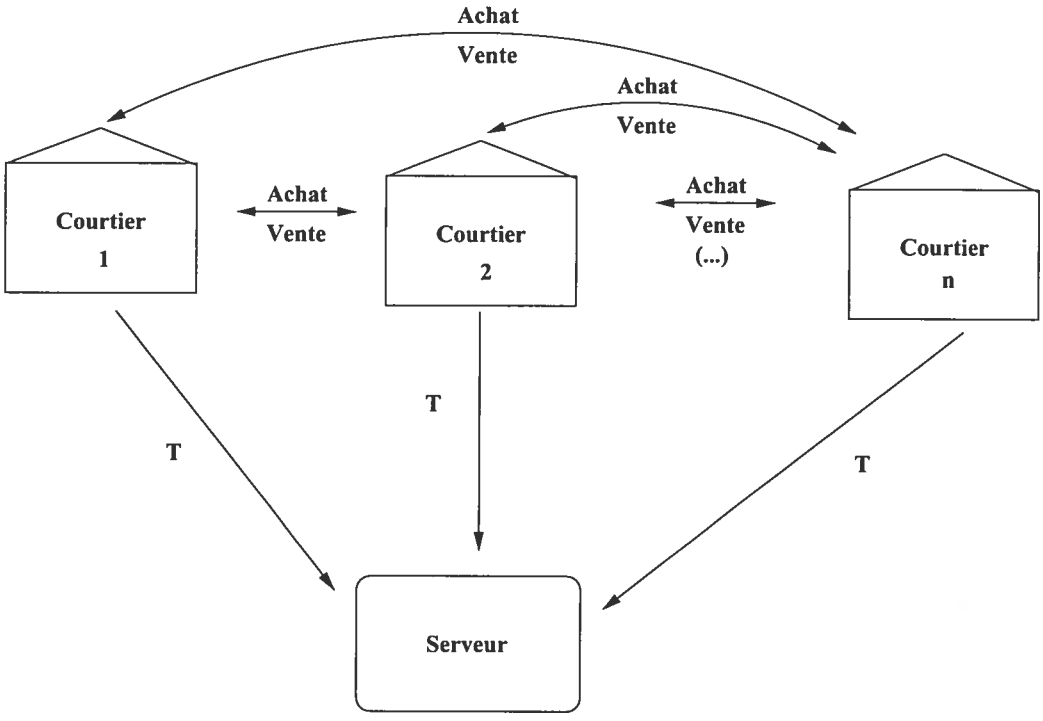


FIG. 2.1 – *Marché institutionnel*

2- Marché hors cote

Les actions des sociétés anonymes qui font un appel public à l'épargne et ne sont pas cotées à la Bourse sont négociées sur le marché hors cote (*Over-the-Counter Market – OTC*). Ce marché est une association de courtiers reliés par des réseaux informatiques et téléphoniques. Un serveur s'occupe d'apparier les offres d'achat et de vente des courtiers. L'investisseur doit communiquer avec son courtier pour acheter ou vendre des titres sur ce marché.

Règle d'échange : il ne peut y avoir d'échange tant qu'une offre d'achat n'est pas jumelée à une offre de vente proposant le même prix pour une même action. Les courtiers exécutent ensuite la transaction au moyen du serveur.



T : Offre d'achat ou de vente

FIG. 2.2 – *Marché hors cote*

3- Marché boursier

Dans un système d'échanges boursiers, l'investisseur cherche à acheter ou à vendre des actions cotées en Bourse. Pour ce faire, il place un ordre d'achat ou de vente chez un courtier dont il est le client; ce contrat l'oblige à payer ou à remettre ses actions si son ordre est apparié.

Définition 2.1. Un *ordre d'achat (de vente)* est une demande d'acheter (de vendre) une ou plusieurs actions d'un titre à un certain prix.

Le courtier (ou la firme de courtage) sert de trait d'union entre l'investisseur et la Bourse. Il est en contact avec des négociateurs (*traders*), c'est-à-dire des personnes qu'il paie pour se trouver sur le parquet de la Bourse et pour placer les ordres de ses clients. Les négociateurs sont les seules personnes admises à la Bourse et doivent être enregistrés à la Bourse pour s'y trouver. Ils sont en contact permanent avec la Bourse, laquelle contrôle les prix courants de tous les titres et gère la liste des ordres placés.

Définition 2.2. Le *prix courant* d'une action est le dernier prix auquel ce titre a été vendu et acheté. Acheter (ou vendre) à prix courant signifie acheter (ou vendre) *immédiatement* au prix courant, quel qu'il soit.

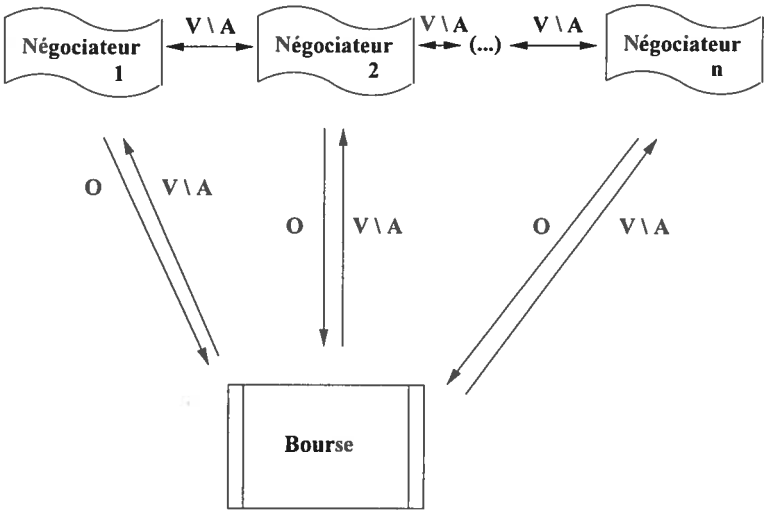
La Bourse maintient une réserve de la majorité des titres, c'est-à-dire qu'elle peut acheter et vendre à son compte certains titres. Elle s'occupe aussi de jumeler les ordres d'achat et de vente; pour un titre, elle trouve un acheteur qui offre un certain prix et un vendeur qui demande ce même prix.

Définition 2.3. On dit qu'un ordre d'achat (de vente) *correspond* à un ordre de vente (d'achat) si ces deux ordres portent sur le même titre et le même prix.

Règles d'échange : Un échange a lieu

- s'il y a un ordre d'achat correspondant à un ordre de vente, c'est-à-dire si les deux ordres proposent le même prix pour le même titre ou
- si le prix de l'ordre correspond au prix courant du titre et si la Bourse garde une réserve de ce titre.

Dans le premier cas, il s'agit d'un échange entre deux négociateurs passant par l'intermédiaire de la Bourse, tandis que dans le second cas, c'est un échange entre un négociateur et la Bourse. Une fois leurs ordres couplés, le ou les négociateurs impliqués sont avisés et doivent soit payer la Bourse, soit lui remettre les actions.



O : Ordre d'achat ou de vente

V \ A : Vente ou achat

FIG. 2.3 – *La Bourse*

2.2 Systèmes d'actions électroniques existants

MacKenzie et Sorensen ont signé le premier article portant sur les systèmes d'actions électroniques anonymes [19]. En utilisant les résultats propres aux systèmes d'argent électronique, ils ont développé un système d'actions électroniques tenant compte de dividendes, de votes et d'impôts. Di Crescenzo, pour sa part, a publié un article décrivant un système d'échanges d'actions électroniques anonymes qui se base sur des résultats propres aux systèmes d'enchères anonymes [10]. Enfin, Ogata et Matsuo, dans leur article [20], appliquent le transfert équivoque aux transactions financières. Les trois articles proposent un système d'échanges boursiers anonymes; cependant, d'après notre analyse, aucun n'est valable, soit parce que le mode d'échange modélisé n'existe pas, soit parce que la sécurité des protocoles n'est pas adéquate.

2.2.1 Le modèle de MacKenzie et Sorensen

Premiers à offrir la définition d'une action électronique anonyme, MacKenzie et Sorensen modélisent un système d'actions électroniques complet où les investisseurs restent anonymes pendant l'échange. Le propriétaire d'une action reste anonyme même après l'achat; il peut recevoir les dividendes, utiliser son droit de vote et payer les impôts de manière anonyme.

Description

Ce système d'actions comporte six entités :

la compagnie : elle administre et vend les actions électroniques;

les investisseurs : ils souhaitent transiger les actions de la compagnie;

la banque : elle utilise le système FOLC pour créer et gérer l'argent électronique utilisé;

l'autorité de certification : elle fournit un ou plusieurs CAPK à tout investisseur désirant rester anonyme en utilisant des protocoles propres au FOLC;

le gouvernement : il collecte les impôts liés aux actions électroniques, tant de l'investisseur que de la compagnie;

une tierce personne de confiance : dans certains cas prédéterminés, elle révoque l'anonymat du propriétaire d'un CAPK.

Une action électronique est une paire « clé publique certifiée et certificat associé » que la compagnie signe et garde dans une base de données publique. On y retrouve (nom de l'action, $sign_C(p, Cert_{CA}(p, X))$) où

- « nom de l'action » est unique et correspond à une action particulière de la compagnie
- $sign_C(.)$ est une signature de la compagnie
- p, $Cert_{CA}(p, X)$ est la paire « clé publique certifiée (p) et certificat associé ($Cert_{CA}(p, X)$) » ; autrement dit, le CAPK

Les investisseurs peuvent consulter librement la base de données des actions sans toutefois connaître les véritables identités associées aux titres.

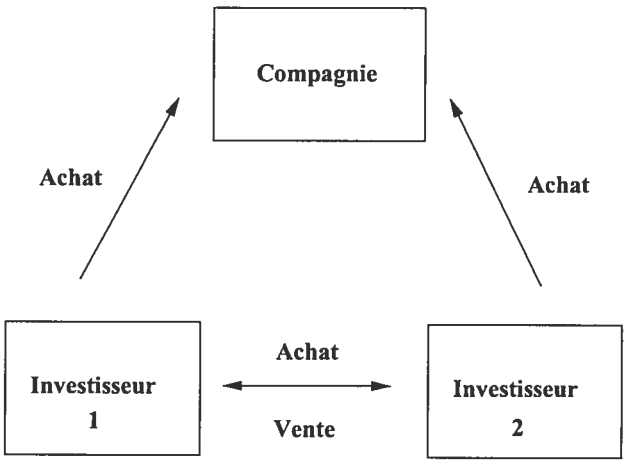


FIG. 2.4 – *Modèle MacKenzie et Sorensen*

Le système comprend quatre protocoles : obtention d'un CAPK, achat d'action à la compagnie, paiement versé par la compagnie à l'investisseur et échange d'action entre deux investisseurs. Les deux derniers protocoles peuvent être utilisés, une fois adaptés, à des fins de compte rendu fiscal. L'investisseur souhaitant transiger anonymement doit commencer par obtenir un CAPK de l'autorité de certification. Pour ce faire, il utilise premièrement le protocole de retrait d'argent électronique pour obtenir, de l'autorité de certification, une pièce (c) de montant nul. Il utilise ensuite le protocole de paiement du FOLC pour payer la certification de sa clé publique (p), qu'il a lui-même générée, à l'aide de la pièce qu'il vient de retirer. L'autorité de certification conserve la pièce reçue (c') et remet un certificat de forme $Cert_{CA}(p, c')$ à l'investisseur. La pièce reçue permet au tiers de confiance de révéler l'identité de la personne qui l'a utilisée lors d'un paiement; ceci découle des propriétés des protocoles du FOLC.

Après avoir obtenu un ou plusieurs CAPK de l'autorité de certification, l'investisseur affiche son offre d'achat ou de vente d'actions sur un babillard anonyme (*Anonymous Bulletin Board*). Cette annonce est signée et peut être cryptée à l'aide des clés associées au CAPK.

Définition 2.4. Un *babillard anonyme* est un réseau de communication anonyme dans lequel les parties peuvent communiquer anonymement deux à deux ou par diffusion.

L'investisseur peut, s'il le désire, acheter une action directement de la compagnie. Il transmet sa demande et son CAPK à la compagnie. Après avoir vérifié la validité de ce CAPK, celle-ci lui transmet un message d'acceptation et fait correspondre au CAPK une action de la base de données publique. L'investisseur paie alors la compagnie en utilisant le protocole de paiement.

L'investisseur peut par contre être intéressé par les offres affichées sur le babillard. Si une offre d'achat (de vente) particulière correspond à sa propre offre

de vente (d'achat), il affiche alors une annonce d'offre de transfert de propriété (de paiement) contenant son CAPK, le CAPK de l'autre investisseur et le prix demandé (offert). Si le second investisseur est intéressé, il affiche un message d'acceptation. Dans tous les cas, la personne qui vend les actions avise la compagnie du transfert de propriété de son action tandis que celle qui achète paie la compagnie. Ensuite, la compagnie paie le vendeur et change le CAPK associé aux actions dans la base de données publique des actions.

En guise de paiement, la compagnie transmet à l'investisseur un chèque électronique portant son CAPK. L'investisseur endosse le chèque et le remet à la banque, qui en vérifie la validité de même que celle du CAPK. Soulignons que l'anonymat de l'investisseur n'est pas compromis, car la banque lui transfère l'argent électronique en utilisant un protocole de retrait au lieu de le déposer dans son compte – compte qui est associé à son identité réelle.

Analyse

Théorème 2.1. *Le système d'échange d'actions proposé par MacKenzie et Sorensen procure un anonymat juste et calculatoire aux investisseurs.*

Démonstration. Ce système d'actions électroniques utilise les protocoles du FOLC pour dissimuler l'identité d'un investisseur à l'intérieur de son CAPK. En effet, l'autorité de certification a recours au protocole de retrait pour cacher l'identité de l'investisseur de manière calculatoire des investisseurs malhonnêtes, de la compagnie, du gouvernement et de la banque; ce faisant, elle ne découvre pas l'identité de l'investisseur. Trouver l'identité de l'investisseur équivaut soit à convaincre le tiers de confiance d'entreprendre le protocole de retracement du propriétaire du FOLC, qui a la propriété d'être efficace, soit à résoudre un problème considéré comme difficile. □

Fait 2.1. *Le système d'échange a comme propriété que les transactions et les actions ne peuvent être reliées entre elles.*

Justification. L'investisseur est anonyme aux yeux de tous mais, s'il utilise le même CAPK à plusieurs reprises, ses transactions peuvent être reliées entre elles. Il lui revient donc de décider s'il veut que ses transactions puissent être corrélées ou non. S'il souhaite l'éviter, il lui faut changer de CAPK à chaque transaction. □

Fait 2.2. *Le système d'échange d'actions de MacKenzie et al. ne modélise aucun mode d'échange d'actions existant.*

Justification. Modélisé comme un système d'échanges où les investisseurs peuvent acheter une action de la compagnie ou se l'échanger entre eux, le système décrit ci-dessus ne reflète aucun des modes d'échanges d'actions possibles. Ce sera un marché hors cote si l'on omet le protocole d'achat d'action entre la compagnie et l'investisseur et si l'on transforme la compagnie en serveur principal et les investisseurs en courtiers. Par contre, si l'on rejette tous les protocoles auxquels participe la compagnie, ne laissant que la possibilité d'échange entre investisseurs, ce système modélise le marché institutionnel. □

Pour que ce système corresponde à un système d'échanges boursiers, il faut éliminer certains protocoles, en ajouter d'autres et redéfinir les parties impliquées. Deux solutions basées sur cet article seront présentées au prochain chapitre.

2.2.2 Le modèle de Di Crescenzo

Di Crescenzo propose un système d'actions plus spécialisé: un système d'opérations boursières. Il considère l'achat et la vente d'un titre d'une seule compagnie. Dans ce système, l'investisseur n'est pas anonyme, ce sont la nature et le contenu de la transaction qui restent privés. En effet, les données telles que le type de transaction (l'achat ou la vente), le nombre d'actions et le prix offert ou demandé ne peuvent être associées à un investisseur en particulier, c'est-à-dire à une identité.

Description

Le système d'échange d'actions est composé d'un serveur honnête mais curieux et d'investisseurs. Le serveur s'occupe de vendre et d'acheter les actions, ainsi que de mettre à jour le nombre d'actions disponibles et leur prix. Les investisseurs interagissent seulement avec le serveur et pas nécessairement en même temps. Ils lui font une proposition dont les détails restent privés : ils lui offrent un prix d'achat ou de vente pour un certain nombre d'actions.

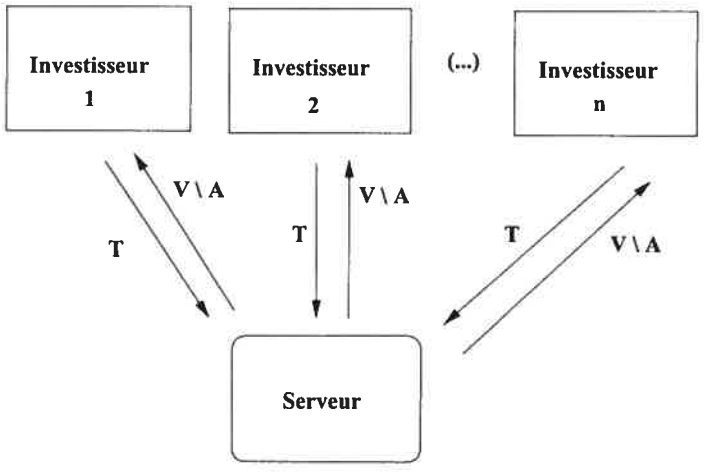


FIG. 2.5 – *Modèle Di Crescenzo*

Ce système définit une action électronique comme étant un certificat signé par le serveur, attestant que le propriétaire du certificat possède une action de la compagnie. Une transaction complète comprend quatre protocoles se déroulant l'un à la suite de l'autre : l'enregistrement, la mise à jour du prix courant du titre, la mise à jour des gains en capital et la certification. Les « valeurs privées » de l'investisseur correspondent aux informations constituant son offre.

Lorsqu'il s'enregistre chez le serveur, l'investisseur reçoit une paire de clés – une publique et une secrète – après avoir fourni une authentification de son identité. Le serveur obtient ensuite une mise en gage des valeurs privées de l'investisseur.

Après un certain lapse de temps, le serveur n'enregistre plus d'investisseurs; il exécute le protocole de mise à jour du prix courant. Di Crescenzo considère que le prix courant ne dépend que de l'ancien prix courant et des valeurs privées des investisseurs. L'auteur propose un protocole très efficace si la fonction permettant d'obtenir le nouveau prix courant est linéaire, protocole basé sur un partage de secret (*secret sharing*) qui inclut tous les investisseurs, c'est-à-dire toutes les valeurs privées. Le protocole devient cependant moins efficace si la fonction est arbitraire. L'auteur propose donc un second protocole pendant lequel chaque investisseur interagit avec le serveur pour échanger des données – données qui ne compromettent pas ses valeurs privées – avec les autres investisseurs et pour effectuer des calculs à l'aide de ces données, par après. Si les résultats des protocoles entre le serveur et chaque investisseur sont les mêmes, le serveur obtient le résultat de la fonction. Quels que soient les fonctions et les protocoles choisis, le serveur ne peut avoir obtenu de l'information sur les données privées des investisseurs pendant le protocole.

Après avoir trouvé le nouveau prix courant, le serveur entame le protocole de mise à jour du nombre d'actions disponibles. Les actions dont le prix d'achat est plus élevé que le prix courant – prix trouvé grâce au protocole précédent – sont vendues, tandis que les actions dont le prix de vente est inférieur au prix

courant sont achetées. En additionnant le nombre d'actions achetées – de poids positif – et celui des actions vendues – de poids négatif – avec le total d'actions qu'il a en réserve, le serveur obtient le nouveau nombre d'actions disponibles. Pour obtenir cette somme, le serveur entreprend un calcul interactif avec les investisseurs consistant en un partage de secret et de preuves à divulgation nulle. Bien qu'il obtienne la somme des valeurs privées des investisseurs qui ont vendu ou acheté des actions, le serveur n'acquiert aucune information supplémentaire sur les valeurs privées et sur leur provenance.

Si l'investisseur a interagi honnêtement avec le serveur pendant les protocoles précédents, il reçoit ensuite un certificat indiquant le prix qu'il avait offert, le type de transaction voulue, le nombre d'actions et le nouveau prix courant de l'action.

Analyse

L'anonymat d'un investisseur, défini ici comme étant l'impossibilité de relier ses données privées à son identité, est calculatoire, car la sécurité du système est basée sur l'hypothèse Diffie-Hellman version décision; démentir cette hypothèse signifie que l'anonymat n'est plus garanti. Ce système a comme particularité qu'une collusion de tous les investisseurs sauf un ne peut obtenir d'information sur les valeurs privées de l'investisseur exclu, même en déviant des protocoles.

Fait 2.3. *Il est faux que le système de Di Crescenzo modélise un système d'échanges boursiers anonymes; en fait, ce système ne modélise aucun mode d'échange existant.*

Justification. Le système d'échanges boursiers de Di Crescenzo est un système de vente aux enchères : les offres d'achat et de vente des investisseurs sont comparées et les actions sont transigées au prix courant seulement. Seuls les investisseurs qui

ont « bien misé » en voulant acheter à un prix plus élevé ou vendre à un prix moins élevé que le prix courant calculé peuvent accomplir la transaction.

Ce système ne modélise pas le marché institutionnel, car les investisseurs achètent et vendent leurs actions au serveur. Il ne modélise pas non plus les marchés hors cote et boursier puisque le rôle du serveur dans ce cas-ci ne correspond pas au rôle qui lui est normalement attribué. Dans ces deux marchés, le serveur sert d'intermédiaire entre deux parties (courtiers ou négociateurs, selon le cas) en appariant leurs ordres d'achat et de vente et, à la Bourse, il peut vendre et acheter des actions à prix courant, s'il en tient une réserve. En aucun cas les parties ne sont contraintes de transiger leurs actions seulement au prix courant et uniquement avec le serveur. □

On remarque aussi que le prix courant calculé dans le protocole de mise à jour du prix courant dépend des offres et du nombre d'actions disponibles, ce qui n'est pas le cas en réalité. Aussi, il faut souligner que le nombre d'actions disponibles à la Bourse dépend des offres de vente des investisseurs et des actions en réserve à la Bourse, s'il y a une réserve du titre en question; il ne se limite pas à la réserve.

2.2.3 Le modèle de Matsuo et Ogata

Matsuo et Ogata sont les premiers à décrire le fonctionnement de la Bourse et à vouloir créer des protocoles pour la modéliser telle qu'elle est. Pour ce faire, ils utilisent une variante du transfert équivoque – le *Matching Oblivious Transfer* – afin de créer des protocoles propres aux échanges boursiers permettant à l'investisseur de rester anonyme et faisant en sorte que les prix des ordres restent inconnus.

Description

Dans ce système, le serveur accepte et publie les ordres d'achat et de vente que placent les investisseurs. Bien qu'il puisse vérifier le contenu d'un ordre, le prix qui y est offert (ou demandé) reste privé. Les investisseurs se chargent de vérifier s'il y a un ordre correspondant au leur (voir la définition 2.3) et, le cas échéant, veillent à récupérer l'argent ou les actions qui leur sont dus.

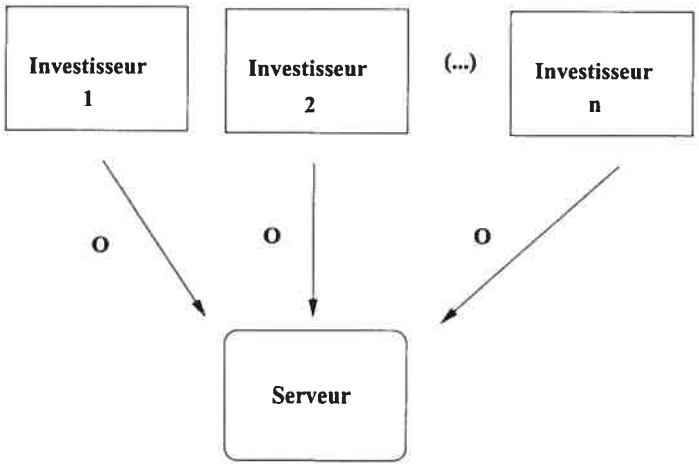


FIG. 2.6 – *Modèle Matsuo et Ogata*

L'offre d'achat de l'investisseur I_j est notée $O_j^{(A)}(m_j)$, où m_j est une pièce d'argent électronique de montant j – le prix offert. L'ordre de vente de ce même investisseur est $O_j^{(V)}(d_j)$, où d_i est l'action électronique à vendre au prix j. Les auteurs de l'article considèrent que le prix d'un titre est compris dans un intervalle prédéterminé et fini; sans perte de généralité, on pose que, pour le prix i, $i \in \{1, \ldots, m\}$. La définition d'une action électronique dans ce contexte est limitée; une action correspond à une donnée numérique, sans autre détail. Pour expliquer les protocoles, on suppose ici qu'un seul titre peut être transigé.

Outre la procédure d'initialisation du serveur qui est accomplie une seule fois, le système compte trois protocoles : un premier pour placer un ordre d'achat, un second pour placer un ordre de vente et un dernier pour récupérer l'argent ou les actions électroniques. Le serveur doit initialiser préalablement des variables pour tous les prix possibles du titre. Ces variables sont en fait un identificateur d'ordre pour chaque prix. Pour $i \in \{1, \ldots, m\}$, il pose $C_i^{(A)} = r_i = C_i^{(V)}$ où r_i est choisi aléatoirement, $C_i^{(A)}$ est un identificateur pour les ordres d'achat correspondant au prix i et $C_i^{(V)}$ est un identificateur pour les ordres de vente correspondant au prix i.

Pour le protocole de placement d'un ordre de vente, le serveur génère des clés publiques pour chaque prix i possible. Pour $C_i^{(V)} = c$, il génère donc $PK_{i,c}^{(V)}$ et $SK_{i,c}^{(A)}$. Pour tous les i, il créé ensuite les clés partielles $SK_{i,c}^{(A)(1)}$ et $SK_{i,c}^{(A)(2)}$ de manière aléatoire en suivant l'égalité suivante :

$$SK_{i,c}^{(A)(1)} + SK_{i,c}^{(A)(2)} = SK_{i,c}^{(A)}.$$

Le serveur prépare aussi une paire $(X(i), sign_S(X(i)))$ où $X(i)$ est une information portant, entre autres, sur le prix indiqué dans l'ordre et s est sa clé privée. Finalement, il pose $T_i = [PK_{i,c}^{(V)}, sign_S(X(i)), SK_{i,c}^{(A)(1)}]$. Après un transfert équivoque (1, m) – OT avec le serveur, l'investisseur I_j, demandant le prix j, reçoit la donnée T_j. L'investisseur crypte l'action qu'il veut vendre, soit d_j, à l'aide de la clé $PK_{j,c}^{(V)}$, le résultat étant O_j. Il transmet cette donnée et les données $(X(j), sign_S(X(j)))$

au serveur. Ce dernier vérifie alors la signature et refait un transfert équivoque (1, m) – OT avec l'investisseur pour que ce dernier obtienne $SK_{i,c}^{(A)(2)}$. Ainsi, l'investisseur peut reconstituer $SK_{i,c}^{(A)}$. Finalement, le serveur insère O_j dans sa base de données d'ordres de vente et met à jour la variable $C_j^{(V)}$: $C_j^{(V)} = C_j^{(V)} \times r_j$.

La description du protocole de placement d'un ordre de vente est similaire.

Pour récupérer l'argent, le protocole est le suivant : à chaque mise à jour de la base de données d'ordres d'achat, l'investisseur ayant placé un ordre de vente décrypte toutes les données et, s'il trouve de l'argent électronique valide, c'est que son ordre a été jumelé. De la même façon, un investisseur ayant placé un ordre d'achat vérifie, à chaque mise à jour de la base de données d'ordres de vente, s'il y a une action électronique valide.

Analyse

Dans ce contexte, on considère que tous les acteurs du système – serveur et investisseurs – peuvent être malhonnêtes et chercher à obtenir de l'information sur les ordres placés ou à obtenir de l'argent ou une action électronique qui ne leur appartient pas.

Théorème 2.2. *Ce système n'est pas sécuritaire face à un serveur malhonnête.*

Démonstration. Les auteurs considèrent qu'en utilisant un transfert équivoque pour placer un ordre, le serveur ne peut découvrir le prix offert (demandé) par l'investisseur. Cependant, l'investisseur envoie des données au serveur qui lui permettent effectivement de connaître le prix en question. En effet, en vérifiant $X(j)$ et $sign_S(X(j))$, le serveur obtient j par l'information contenue dans $X(j)$. De plus, s'il a gardé en mémoire tous les T_j, il peut trouver, à l'aide de $X(j)$, la valeur j et même les clés publique et privées correspondantes. Avec ces clés en main, le

serveur peut s'approprier les actions et l'argent électronique que les investisseurs lui confient pour qu'ils soient insérés dans la base de données publique. □

Théorème 2.3. *La sécurité des données numériques face aux investisseurs malhonnêtes est calculatoire.*

Démonstration. Les données numériques sont publiées une fois qu'elles ont été cryptées à l'aide d'une clé publique. Pour obtenir ces données, il faut donc avoir la clé secrète correspondante. Obtenir ces données malicieusement correspond à résoudre le problème Logarithme discret. □

Bref, ce système n'est pas sécuritaire face à un serveur malhonnête. Néanmoins, les prix offerts ou demandés restent inconnus des investisseurs malhonnêtes et ces derniers ne peuvent s'approprier des données qui ne leur appartiennent pas, car connaître un prix ou décrypter une donnée qui ne leur est pas destinée équivaut à résoudre un problème considéré comme difficile.
En plus des déficiences au niveau de la sécurité, ce système comporte plusieurs problèmes importants :

i. Le serveur ne vérifie pas si l'argent ou l'action que veut échanger l'investisseur est valide.

ii. En supposant que les prix restent privés – inconnus du serveur et des autres investisseurs – dans ce modèle, le prix courant d'un titre, qui est une information essentielle à tout investisseur, ne peut être connu.

iii. L'investisseur ne peut retirer son ordre lorsque celui-ci a été placé.

iv. Le transfert équivoque entre le serveur et l'investisseur dépend de l'honnêteté de l'investisseur. Celui-ci peut, s'il le désire, choisir une clé publique ne correspondant pas au prix qu'il a offert ou demandé. Par exemple, il peut obtenir un montant d'argent plus élevé que celui qu'il avait demandé.

2.3 Analyse globale des systèmes

Les systèmes transactionnels anonymes proposés suggèrent deux façons de préserver l'anonymat d'un investisseur. En effet, MacKenzie et Sorensen proposent de cacher l'identité de l'investisseur tandis que Di Crescenzo et Matsuo et Ogata suggèrent plutôt de rendre privé le contenu d'une transaction, c'est-à-dire ses données essentielles. La différence entre ces deux stratégies repose sur le fait que, dans le premier cas, on fait en sorte que l'identité de l'utilisateur puisse être retrouvée avec l'aide d'un tiers de confiance et que, dans les deux autres cas, le contenu ne peut être retrouvé sans résoudre un problème difficile.

Dissimuler le contenu n'est pas la meilleure stratégie pour modéliser un système boursier. Il est essentiel de divulguer les prix offerts, demandés et courants, car la connaissance de ces prix est indispensable pour la prise d'une décision d'investissement et pour le bon fonctionnement des marchés boursier et financier. Comme nous l'avons signalé, aucun de ces systèmes ne modélise vraiment un système d'échanges boursiers anonymes. Il s'agit donc de créer un tel système en tenant compte des caractéristiques propres à la Bourse, du besoin de rendre les transactions anonymes et des limites que doit posséder cet anonymat.

Modèle	Mode d'échange annoncé	Mode d'échange modélisé	Donnée(s) privée(s)	Tiers de confiance	Sécurité : compagnie	Sécurité : serveur	Sécurité : investisseurs
MacKenzie *et al.*	quelconque	**aucun**	identité de l'investisseur	oui	calculatoire et révocable	S/O	calculatoire et révocable
Di Crescenzo	boursier	**aucun**	prix, nombre d'actions, type de transaction	non	S/O	calculatoire	calculatoire
Matsuo et Ogata	boursier	boursier	prix	non	S/O	**aucune**	calculatoire

TAB. 2.1 – *Comparaison des systèmes d'actions électroniques présentés*

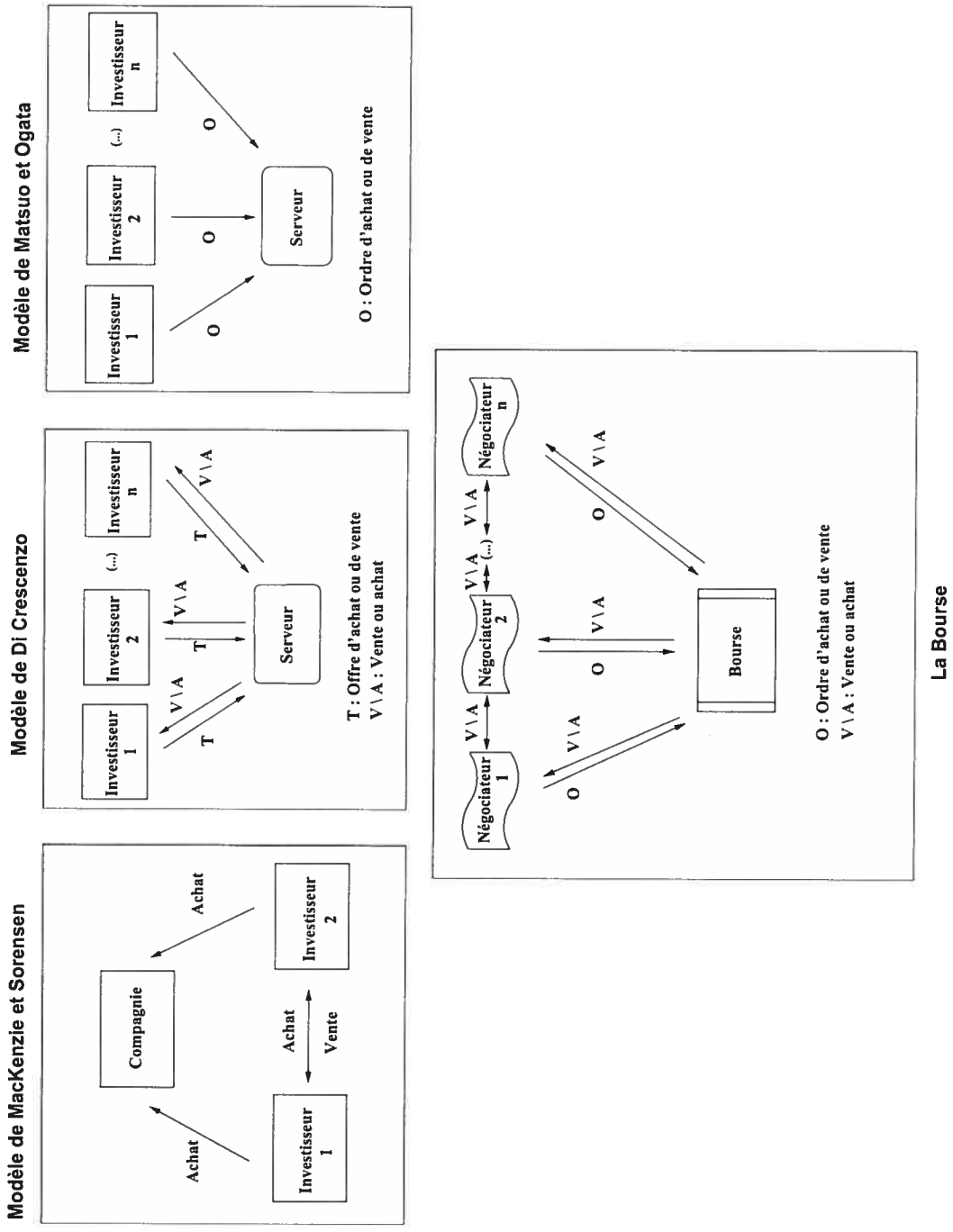


FIG. 2.7 – *Comparaison schématique des modèles présentés*

Chapitre 3

Échanges boursiers anonymes: nos solutions

3.1 Motivation

Présentement, lors de transactions boursières, l'auteur d'une infraction grave – non-paiement ou fraude, par exemple – est facilement identifiable qu'il soit courtier, négociateur ou investisseur. Le négociateur doit être enregistré à la Bourse pour s'y trouver et l'investisseur doit fournir des renseignements personnels dès le premier contact avec son courtier. Ainsi, tous les actes qu'ils posent peuvent être retracés jusqu'à eux.

Une telle visibilité est justifiée pour limiter la criminalité. Le revers de la médaille est que cette visibilité permet aux courtiers et aux négociateurs de connaître et d'analyser les agissements des autres et surtout d'en profiter. Par exemple, si une institution financière réputée telle une banque demande à son courtier de vendre 100 000 actions de l'entreprise X, celui-ci peut déduire de cette information que, de l'avis de la banque, les actions de X sont surévaluées. Il avise alors ses autres clients de cette vente. De même, voyant un négociateur associé à une certaine firme de courtage vendre 100 000 actions de X, les autres négociateurs peuvent en arriver à la même conclusion : les actions sont surévaluées. Réagissant à la demande

de vente de la banque, d'autres investisseurs et courtiers choisissent de vendre, de sorte que le prix de l'action de X fluctue suffisamment pour désavantager la banque. Ainsi, ils profitent des connaissances financières et des informations que la banque a durement obtenues. Il serait donc utile de cacher l'identité des investisseurs et des négociateurs pour éviter de telles fuites d'information.

De plus, l'association directe entre l'identité d'une personne et ses investissements permet d'établir un dossier; l'investisseur est à jamais lié aux erreurs qu'il a commises. Celles-ci peuvent le discréditer et biaiser les conseils financiers qu'il reçoit. Cette analyse des actions antérieures est une raison motivant l'investisseur à rester anonyme par rapport à son courtier. Celui-ci veut cependant une assurance – une authentification – de l'identité de l'investisseur avant qu'il ne devienne son client, car il ne veut pas faire affaires avec des criminels ou des personnes auxquelles l'accès à la Bourse est interdit.

Le présent projet consiste donc à créer un système électronique d'échanges boursiers anonymes à l'épreuve des fuites d'information et de l'espionnage et qui offre un niveau de sécurité adéquat pour toutes les parties concernées, en tenant compte des résultats et des problèmes mentionnés au chapitre précédent.

3.2 Description du problème

Le problème peut être énoncé comme suit : il s'agit de concevoir un système d'échange d'actions électroniques modélisant les échanges boursiers et offrant, pour ceux qui le désirent, la possibilité de rester anonyme. Un bon système permet aux entités anonymes de le rester pendant et après les protocoles et considère que *tous* les acteurs peuvent vouloir obtenir une identité dissimulée. Pour résoudre le problème, il faut des acteurs, des protocoles et des règles d'échange et de sécurité; tous seront présentés dans cette section.

3.2.1 Les acteurs et leur rôle

Un système d'échanges boursiers comporte les entités suivantes :

- la banque : elle crée et gère de l'argent électronique ainsi que des comptes bancaires.
- la Bourse : elle s'occupe de prendre et de retirer les ordres, se charge d'apparier les ordres, gère les échanges et possède une réserve de certains titres.
- les courtiers : ils restent en contact avec leurs clients, qui leur demandent de placer ou de retirer un ordre, et avec leur négociateur, pour lui transmettre les demandes.
- les clients : ils communiquent avec leur courtier pour placer ou retirer un ordre et possèdent un compte bancaire.
- les négociateurs : selon les demandes de leur courtier attitré, ils placent ou retirent des ordres à la Bourse.

3.2.2 Protocoles requis

Le système électronique d'échanges boursiers anonymes doit comprendre certains protocoles essentiels au bon fonctionnement de la Bourse. Il faut que le client puisse placer un ordre chez son courtier et qu'il puisse le retirer par la suite, s'il le désire. De même, le négociateur doit être en mesure de placer un ordre à la Bourse et de le retirer ensuite. La Bourse, pour sa part, doit pouvoir jumeler les ordres correspondants. Finalement, il doit y avoir un moyen pour les négociateurs, la Bourse, le courtier et les clients d'échanger les actions électroniques et l'argent électronique. Les protocoles peuvent se diviser en deux catégories : protocoles entre le courtier et son client et protocoles entre le négociateur et le serveur. Il n'est pas nécessaire d'élaborer des protocoles entre le courtier et le négociateur, car ceux-ci ne cachent pas leur identité. Leurs communications peuvent avoir lieu sur un canal privé réservé ou sur un canal authentifié.

Les protocoles du système doivent inspirer la confiance aux parties intéressées. Les entités qui souhaitent rester anonymes veulent que leur identité soit protégée

contre les entités malhonnêtes désirant la découvrir ou l'usurper. Par contre, le courtier veut pouvoir vérifier si l'investisseur anonyme est un de ses clients et la Bourse veut pouvoir s'assurer que le négociateur anonyme est enregistré.

Les transactions boursières doivent se dérouler normalement; en particulier, le prix courant de chaque titre doit être disponible. Les actes criminels comme le vol, ainsi que la copie et la double utilisation de données numériques ne doivent pas être possibles.

3.2.3 Anonymat

Pour ne pas compromettre l'anonymat assuré par les protocoles d'échanges boursiers, une action électronique doit être définie comme étant anonyme, l'argent électronique du système choisi doit aussi être anonyme et les communications entre courtier et investisseur et entre négociateur et la Bourse doivent avoir lieu sur des canaux anonymes.

L'anonymat est réservé aux clients et aux négociateurs; quant au courtier, il n'est ni nécessaire ni utile de dissimuler son identité. Lorsque le client anonyme place une demande d'achat ou de vente chez son courtier, celui-ci ne connaît pas son identité; le négociateur et la Bourse l'ignoreront également. Après l'appariement de son ordre, le client souhaite préserver son anonymat pendant la prochaine étape, soit le transfert à son courtier de l'argent ou des actions électroniques correspondant à son ordre.

Le courtier et le négociateur se connaissent, mais la Bourse et les autres négociateurs ne doivent pas découvrir l'identité du négociateur ni pendant qu'il place un ordre, ni pendant l'échange d'argent ou d'actions, le cas échéant.

3.2.4 Propriétés

Le système d'échange d'actions électroniques doit suivre les règles d'échanges suivantes :

R1 : la Bourse jumelle deux ordres correspondants si ceux-ci proposent le même prix pour le même titre;

R2 : si le prix indiqué sur l'ordre correspond au prix courant du titre et si la Bourse garde une réserve de ce titre, elle jumelle l'ordre avec le sien;

R3 : les ordres sont horodatés; donc, si un ordre est placé avant un ordre équivalent, l'ordre placé en premier a priorité sur le second lors de l'appariement;

R4 : un ordre peut être retiré n'importe quand avant d'être jumelé.

Tout comme un système d'argent électronique, un système d'échange d'actions électroniques doit être juste pour éviter les crimes parfaits: il doit comporter un mécanisme de retracement. En plus d'imiter la réalité de la Bourse, les protocoles d'échange proposés devront respecter les règles de sécurité suivantes :

S1 : le client légitime est anonyme;

S2 : le négociateur légitime est anonyme;

S3 : le vendeur n'obtient que de l'argent numérique correspondant à son ordre de vente et l'acheteur n'obtient qu'une action numérique pour son ordre d'achat et cela, seulement une fois les deux ordres jumelés;

S4 : seul le client qui a demandé de placer un ordre peut demander de le retirer;

S5 : seul le négociateur qui a placé l'ordre à la Bourse peut en demander le retrait;

S6 : l'anonymat du client et du négociateur peut être facilement révoqué;

S7 : les protocoles sont sécuritaires face à toutes les entités malhonnêtes, même s'il y a collusion.

Tous les acteurs sauf la banque peuvent être malhonnêtes : ils peuvent chercher à découvrir l'identité d'une entité anonyme ou à s'approprier des données numériques qui ne leur appartiennent pas. Il faut que des règles soient établies pour faire échec

à leur malhonnêteté. Le système d'échange d'actions électroniques doit donc avoir certaines propriétés essentielles :

H1 Une action électronique n'est pas falsifiable: une entité ne peut créer une action sans l'aide de la Bourse.

H2 Une action électronique ne peut être vendue en double: si une entité vend une action en double, son identité est révélée.

Dans la suite de ce document, le problème de modélisation d'un système d'échanges boursiers anonymes sera divisé en deux parties : les protocoles entre le courtier et l'investisseur et ceux entre le négociateur et la Bourse. Dans les solutions qui suivront, l'accent sera mis sur les protocoles transactionnels, car ils sont au coeur des échanges boursiers. Nous ne nous intéresserons donc pas aux protocoles concernant les dividendes, les votes et les retenues fiscales, qui existent toutefois.

3.3 Première solution: un modèle basé sur celui de MacKenzie et Sorensen

La première solution que nous avons envisagée procure un anonymat calculatoire et révocable aux négociateurs et aux investisseurs. Elle apporte des changements au modèle de MacKenzie et Sorensen tout en conservant ses propriétés de sécurité. Le système qui en résulte confirme les hypothèses et respecte les règles d'échange et de sécurité associées à un système d'échanges anonymes pour la Bourse.

3.3.1 Acteurs

Au modèle de MacKenzie et Sorensen s'ajoutent le négociateur, la Bourse et le courtier. De plus, la compagnie est éliminée et nous redéfinissons le rôle de l'investisseur. Aucun changement n'est apporté aux rôles de la banque, du tiers de confiance et de l'autorité de certification.

Le négociateur « N » inscrit à la Bourse se procure un CAPK, place ses ordres à la Bourse et transige avec elle lorsqu'un de ses ordres a été jumelé.

La Bourse s'occupe de prendre et de retirer les ordres des négociateurs enregistrés à la Bourse, de vérifier la légitimité des ordres placés, de jumeler ordres d'achat et ordres de vente d'une même action et de communiquer cette information aux propriétaires, de transférer la propriété des actions, ainsi que de vendre et d'acheter elle-même des actions à prix courant. De plus, elle agit comme intermédiaire dans le paiement entre deux négociateurs. Elle entretient également trois bases de données publiques : une qui contient toutes les actions existantes et le CAPK de leurs propriétaires, une autre les ordres placés et la dernière, les clés publiques des négociateurs enregistrés à la Bourse.

Le courtier accepte les demandes d'achat et de vente de ses clients, vérifie leur contenu, authentifie leurs propriétaires et transfert la propriété des actions. Il tient une liste des clés publiques de ses clients, à laquelle ceux-ci ont accès.

L'investisseur « I» est un client du courtier auquel il demande d'acheter ou de vendre des actions et avec lequel il transige par la suite, s'il y a lieu.

3.3.2 Généralités

À la Bourse, une action électronique est une paire « clé publique certifiée et certificat associé » – un CAPK – signée par la Bourse et conservée dans sa base de données publique où sont listées les actions et que les négociateurs peuvent consulter librement. Pour l'investisseur, une action électronique est une attestation signée par le courtier, prouvant qu'il est bien le propriétaire de l'action associée à un négociateur donné. Puisqu'un CAPK est anonyme et que quiconque, sans restriction, peut en obtenir un, notre modèle tient en compte que le négociateur et l'investisseur doivent chacun fournir une preuve – le négociateur à la Bourse et l'investisseur au courtier – avant de placer un ordre, pour établir qu'ils sont respectivement un membre enregistré et un client.

Tout comme Mackenzie *et al.*, nous supposons que les protocoles d'argent électronique utilisés sont ceux du FOLC. Le protocole d'obtention d'un CAPK est le seul protocole qui reste intacte, inaffecté par les changements apportés au contexte; l'investisseur et le négociateur utilisent ce protocole.

Notons que les communications entre les investisseurs et le courtier, ainsi qu'entre les négociateurs et la Bourse ont lieu sur des canaux anonymes au lieu de babillards anonymes, car ces canaux et les bases de données publiques de demandes et d'ordres placés jouent ensemble le rôle du babillard.

3.3.3 Protocoles

Les notations suivantes seront employées pour la description des protocoles.

- d, le prix demandé ou offert
- C, de l'information sur la transaction, incluant le type de transaction (achat ou vente) et le type d'action
- $\sigma_k^{(i)}$, le numéro d'identification de l'ordre k du négociateur N_i
- $\rho_k^{(i)}$, le numéro d'identification du retrait de l'ordre k du négociateur N_i
- $\delta_n^{(o)}$, le numéro d'identification de la demande n de l'investisseur I_o
- $\varrho_n^{(o)}$, le numéro d'identification du retrait de la demande n de l'investisseur I_o

- s_i, la clé privée associée à p_i
- r, le nombre de négociateurs enregistrés à la Bourse
- t, le nombre de clients du courtier
- $\{p_1, \ldots, p_r\}$, l'ensemble des clés publiques des négociateurs enregistrés à la Bourse
- $\{\overline{p}_1, \ldots, \overline{p}_t\}$, l'ensemble des clés publiques des clients du courtier

Le négociateur et l'investisseur n'exécutent qu'une fois le protocole d'initialisation avant les autres protocoles, afin que l'investisseur s'inscrive auprès du courtier et le négociateur auprès de la Bourse, fournissant ainsi leur véritable identité, de même que leur véritable clé publique. Ensuite, ils se procurent chacun un CAPK. Nous supposons que le négociateur N_i possède (p_i, s_i, $Cert_A(p_i, X_i)$), que l'investisseur I_o possède (p_o, s_o, $Cert_A(p_o, X_o)$), que le courtier possède (p_C, s_C) et que la Bourse possède (p_B, s_B). Les autres protocoles sont les suivants.

Protocole de placement d'un ordre à la Bourse

Pour la demande $\delta_n^{(o)}$, l'investisseur I_o crée la variable *Demande*, où *Demande* $= [\underline{C}, d, p_o, Cert_A(p_o, X_o), \delta_n^{(o)}]$ et $\underline{C}$ contient, entre autres, le type de transaction demandée, le nom de l'action et, dans le cas d'une vente, le CAPK du négociateur associé à l'action. Cela signifie que I_o désire acheter une action au prix d avec $(p_o, Cert_A(p_o, X_o))$ ou vendre au prix d l'action associée au CAPK donné dans $\underline{C}$. I_o produit et remet au courtier une signature en anneau sur *Demande*, construite à l'aide des clés $(\overline{p}_1, \ldots, \overline{p}_t)$ Le courtier archive la demande et communique avec le négociateur N_i pour qu'il place un ordre correspondant à la Bourse.

Soit l'ordre $\sigma_k^{(i)}$ correspondant à $\delta_n^{(o)}$. N_i génère une signature en anneau sur la variable *Offre* en utilisant les clés $(p_1, \ldots, p_r)$, où *Offre* $= [C, d, p_i, Cert_A(p_i, X_i), \sigma_k^{(i)}]$, et la fait parvenir à la Bourse. Selon le contenu de C, cet ordre signifie que N_i désire acheter une action au prix d avec $(p_i, Cert_A(p_i, X_i))$ ou vendre l'action associée à $(p_i, Cert_A(p_i, X_i))$ au prix d. La Bourse vérifie la validité de la signature en anneau et de son contenu, c'est-à-dire $Cert_A(p_i, X_i)$, et ajoute $\sigma_k^{(i)}$ à la base de données publique des ordres placés.

$\mathbf{I_o}$		**Courtier**
	$(Demande, (\overline{p}_1, ..., \overline{p}_t;\ v;\ x_1, ..., x_t))$ $\longrightarrow$	
		Vérifie et archive $(Demande, (\overline{p}_1, ..., \overline{p}_t;\ v;\ x_1, ..., x_t))$
$\mathbf{N_i}$		**Bourse**
	$(Offre, (p_1, ..., p_r;\ v';\ x'_1, ..., x'_r))$ $\longrightarrow$	
		Vérifie $(Offre, (p_1, ..., p_r;\ v';\ x'_1, ..., x'_r))$ Archive $\sigma_k^{(i)}$

TAB. 3.1 – *Placement d'un ordre à la Bourse*

Protocole d'achat (ou de vente) d'une action à prix courant à la Bourse

Si l'ordre $\sigma_k^{(i)}$ est au prix courant, qu'aucun autre ordre ne peut lui être jumelé et que la Bourse maintient une réserve de l'action en question, N_i peut se procurer l'action ou s'en défaire immédiatement, selon le cas. Supposons alors que la Bourse détient des titres de cette action. La Bourse envoie la signature numérique $sign_{s_B}(Entente)$ à N_i, où $Entente = [C', d, Cert_A(p_i, X_i), \sigma_k^{(i)}]$ et C' contient le nom de l'action.

Si $\sigma_k^{(i)}$ est un achat, N_i se procure de l'argent électronique de montant d à la banque. Il exécute ensuite le protocole de paiement avec la Bourse. Une fois le paiement effectué, la Bourse signe $(p_i, Cert_A(p_i, X_i))$ et change le propriétaire de l'action dans la base de données. Si $\sigma_k^{(i)}$ est une vente, N_i et la Bourse exécutent le « protocole de paiement entre la Bourse et le négociateur ». Ensuite, la Bourse s'indique comme étant la propriétaire de l'action dans la base de données.

$\mathbf{N_i}$		**Bourse**
	$sign_{s_B}(Entente)$ $\longleftarrow$	
Achat:	*paiement de* d *dollars* $\longleftrightarrow$	
		Archive $sign_{s_B}(p_i, Cert_A(p_i, X_i))$
Vente:	*«Paiement entre la Bourse et le négociateur»* $\longleftrightarrow$	

TAB. 3.2 – *Achat (ou vente) d'une action à prix courant à la Bourse*

Protocole de paiement entre la Bourse et le négociateur

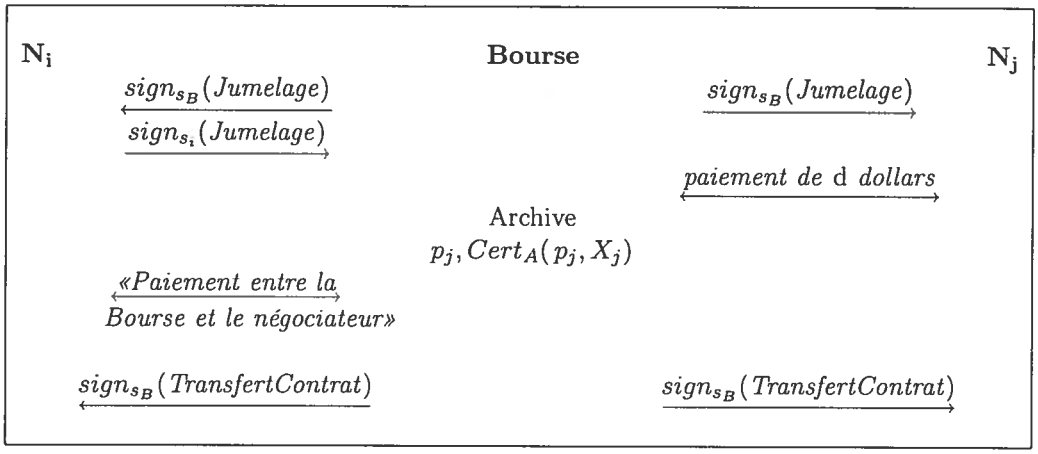
Afin de payer le montant d à N_i, la Bourse obtient de la banque de l'argent électronique de montant d pour réaliser ensuite le protocole de paiement avec N_i. N_i fournit à la banque $(p_i, Cert_A(p_i, X_i))$. La banque vérifie et garde $Cert_A(p_i, X_i)$ avant d'effectuer le protocole de dépôt, puis le protocole de retrait avec N_i. Ce dernier acquiert une pièce de montant d.

$\mathbf{N_i}$		**Bourse**
	paiement de d *dollars* $\longleftrightarrow$	
$\mathbf{N_i}$		**Banque**
	$p_i, Cert_A(p_i, X_i) \longrightarrow$	
		Vérifie et archive $p_i, Cert_A(p_i, X_i)$
	dépôt de d *dollars* $\longleftrightarrow$	
	retrait de d *dollars* $\longleftrightarrow$	

TAB. 3.3 – *Paiement entre la Bourse et le négociateur*

Protocole d'échange d'une action entre deux négociateurs

Quand deux ordres placés par deux négociateurs distincts sont appariés, au prix courant ou non, la Bourse transmet aux deux négociateurs $sign_{s_B}(Jumelage)$, où $Jumelage = [C'', d, Cert_A(p_i, X_i), \sigma_k^{(i)}, Cert_A(p_j, X_j), \sigma_m^{(j)}]$ et C'' comprend le nom de l'action et le CAPK de son propriétaire actuel. Cela signifie que les ordres $\sigma_k^{(i)}$ et $\sigma_m^{(j)}$ des négociateurs N_i et N_j ont été jumelés. Il va de soi que la validité des certificats a été établie par la Bourse préalablement à son message. Sans perte de généralité, le vendeur de l'action est N_i. Il remet à la Bourse $sign_{s_i}(Jumelage)$. L'acheteur N_j paie la Bourse le montant d (il retire de l'argent électronique de montant d à la banque et entame le protocole de paiement avec la Bourse). La Bourse change la propriété de l'action de $(p_i, Cert_A(p_i, X_i))$ à $(p_j, Cert_A(p_j, X_j))$ et effectue le « protocole de paiement entre la Bourse et le négociateur » avec N_i. Elle envoie $sign_{s_B}(TransfertContrat)$ aux deux négociateurs concernés, où $TransfertContrat = [C'', Cert_A(p_j, X_j)]$, comme preuve que le transfert a été fait.

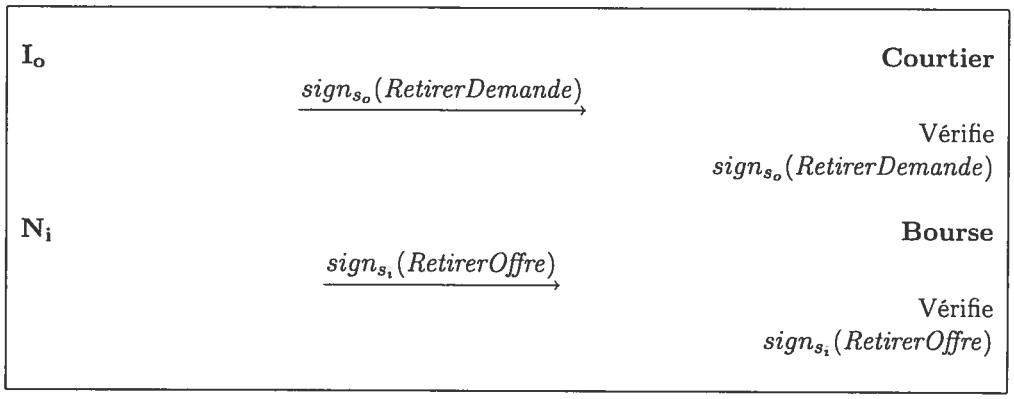


TAB. 3.4 – *Échange d'une action entre deux négociateurs*

Protocole de retrait d'un ordre à la Bourse

Pour retirer la demande $\delta_n^{(o)}$, I_o transmet la signature $sign_{s_o}(RetirerDemande)$, avec $RetirerDemande = [\varrho_n^{(o)}, Demande]$ à son courtier, où s_o est la clé privée associée à p_o, la clé du CAPK contenu dans la variable *Demande* de la demande en question. Après avoir validé la signature, le courtier communique avec le négociateur.

Soit l'ordre $\sigma_k^{(i)}$ correspondant à $\delta_n^{(o)}$. Pour que la Bourse retire cet ordre de la base de données des ordres placés, N_i remet $sign_{s_i}(RetirerOffre)$ à la Bourse, où $RetirerOffre = [\rho_k^{(i)}, Offre]$ et s_i est la clé privée associée à p_i du CAPK contenu dans la variable *Offre* de l'ordre en question. N_i peut ensuite s'assurer que le retrait a été effectué en consultant la base de données des ordres placés.



TAB. 3.5 – *Retrait d'un ordre à la Bourse*

Protocole d'échange entre l'investisseur et le courtier

Dans le cas d'un achat, pour transférer la propriété d'une action du négociateur à l'investisseur I_o, le courtier produit la signature $sign_{s_c}[sign_{s_B}(TransfertContrat), p_o, Cert_A(p_o, X_o), \delta_n^{(o)}]$ où p_o est la clé de I_o associée à la demande d'achat ou de vente dont le numéro d'identification est $\delta_n^{(o)}$. La valeur $sign_{s_B}(TransfertContrat)$ a été reçue par le négociateur pendant la transaction concernant la demande en question. Ainsi, I_o a une attestation prouvant qu'il est propriétaire de l'action. Il utilise ensuite p_o et $Cert_A(p_o, X_o)$ pour exécuter le protocole de paiement avec le courtier. Dans le cas d'une vente, I_o transmet au courtier la valeur qu'il a reçue lors de l'achat de l'action, soit $sign_{s_c}[sign_{s_B}(TransfertContrat),\ p_o, Cert_A(p_o, X_o), \delta_n^{(o)}]$. Le courtier vérifie qu'elle figure dans ses archives et, le cas échéant, la retire. Ils procèdent ensuite au le protocole de paiement.

$\mathbf{I_o}$		**Courtier**
Achat:	$\xleftarrow{sign_{s_c}[sign_{s_B}(TransfertContrat),\ p_o, Cert_A(p_o, X_o), \delta_n^{(o)}]}$	
	$\xleftrightarrow{paiement\ de\ \mathrm{d}\ dollars}$	
Vente:	$\xrightarrow{sign_{s_c}[sign_{s_B}(TransfertContrat),\ p_o, Cert_A(p_o, X_o), \delta_n^{(o)}]}$	
	$\xleftrightarrow{paiement\ de\ \mathrm{d}\ dollars}$	

TAB. 3.6 – *Échange entre l'investisseur et le courtier*

3.3.4 Analyse

Fait 3.1. *Ce système possède les deux propriétés des actions électroniques anonymes.*

Justification. (H1) Une action est falsifiée lorsqu'elle est vendue par une entité qui n'en est pas le propriétaire. Celle-ci doit en effet produire une signature numérique valide pour des données auxquelles elle n'a pas accès et utiliser une clé de signature qu'elle ne connaît pas. En fait, elle doit soit deviner la signature, soit résoudre un problème jugé difficile (problème dépendant de l'infrastructure à clé publique employée). (H2) Vendre une action en double revient à falsifier une action, car l'entité vend alors une action qui ne lui appartient plus. □

Fait 3.2. *Les protocoles possèdent toutes les propriétés de sécurité énoncées à la section 3.2.4.*

Justification. (S1 et S2) Un client (négociateur) est légitime si la signature en anneau fournie avec sa demande (son ordre) est valide. Produire une telle signature sans appartenir au groupe auquel il s'est identifié au moment de la signature équivaut soit à deviner la signature, soit à inverser une fonction à sens unique avec brèche secrète – un problème difficile. Un client (négociateur) légitime reste anonyme pendant et après les protocoles, car le CAPK et, s'il en utilise, l'argent électronique lui procurent un anonymat calculatoire et révocable. Son identité ne peut être connue que si un tiers de confiance accepte de la divulguer. (S3) Une entité obtient une action qui ne lui appartient pas si elle falsifie une action. Elle obtient de l'argent numérique qui ne lui appartient pas si elle fournit une signature numérique valide, ne connaissant ni les données à signer ni la clé de signature. (S4 et S5) Le retrait d'un ordre aussi nécessite une signature numérique; la sécurité du protocole de retrait dépend donc également du type de signature utilisé. (S6) Il n'est pas possible d'obtenir un CAPK qui n'est pas associé à une véritable identité et qui n'a pas été créé par l'autorité de certification, car la signature de l'autorité

de certification et les pièces d'argent électronique du FOLC ont la propriété de ne pas pouvoir être forgés. En effet, forger un CAPK signifie forger une signature numérique de Schnorr et une pièce FOLC (propriété P5 du FOLC). Les propriétés du CAPK et la propriété P4 du FOLC font en sorte que l'anonymat d'une entité ayant un CAPK peut être facilement révoqué. (S7) Une fois un ordre jumelé, une entité qui ne paie pas ou ne cède pas l'action en question sera retracée, même si elle agit malhonnêtement en collusion avec la Bourse. La base de données des ordres placés permet de vérifier les agissements de la Bourse; par exemple, si elle n'associe pas deux ordres devant être jumelés, tout négociateur peut s'en rendre compte. Si elle ne change pas la propriété de l'action ou ne paie pas le vendeur de l'action, elle sera réprimandée puisque le négociateur a pour preuve la transcription du protocole qu'il a effectué et la base de données des actions et de leur propriétaire. L'investisseur et le négociateur sont protégés des collusions contre eux, car toute entité voulant leur nuire doit forger soit leur signature numérique, soit une pièce de FOLC. □

Théorème 3.1. *Ce système d'échanges boursiers anonymes procure aux entités qui le désirent un anonymat calculatoire et révocable. Si elle le souhaite, une entité peut s'assurer que ses transactions ne peuvent être reliées entre elles.*

Théorème 3.2. *La sécurité des protocoles d'achat d'une action de la Bourse ou de vente d'une action à la Bourse, d'échange entre deux négociateurs ainsi que de retrait d'un ordre est calculatoire et dépend de la sécurité de l'infrastructure à clé publique, plus précisément de la signature numérique associée à cette infrastructure.*

Théorème 3.3. *La sécurité de ce système d'échanges est calculatoire face à la Bourse, aux négociateurs, aux courtiers et aux investisseurs malhonnêtes, en collusion ou non.*

3.4 Deuxième solution: un modèle basé sur celui de MacKenzie et Sorensen et sur celui de Xu, Yung et Zhang

Dans les modèles de MacKenzie et Sorensen et de la solution précédente, une seule action peut être transigée à la fois. Pour vendre 1000 actions, l'investisseur et le négociateur doivent chacun générer 1000 signatures et le courtier de même que la Bourse doivent chacun vérifier 1000 de ces signatures et les 1000 CAPK correspondant aux actions en question. Le système boursier se caractérise par la succession rapide des transactions et leur volume élevé en une journée. La deuxième solution que nous proposons est une adaptation du système de Xu, Yung et Zhang [18]. Elle est plus fonctionnelle puisque le nombre d'actions transigées n'influe pas sur l'opération.

3.4.1 Généralités

Pour permettre de bien saisir les protocoles cryptographiques de cette solution, deux concepts sont décrits: la signature numérique à l'encre magique (*magic ink signature*) et la cryptographie proactive (*proactive cryptography*).

La signature à l'encre magique [16] est une signature à l'aveugle distribuée: elle est produite par un quorum de signataires et le message peut être démasqué plus tard par un autre quorum de signataires, selon des règles préétablies. S'il y a n entités de confiance,

- une signature à l'encre magique valide est générée par t, $0 \leq t \leq n$, des n entités de confiance, car s'il y a moins de t signataires, la signature ne peut être valide;
- le message ne peut être démasqué par moins de t entités;
- le message peut être démasqué par t des n entités, qu'elles aient eu ou non un rôle dans la génération de la signature et quel que soit le comportement des $n - t$ autres entités.

Un adversaire compromettant la clé secrète de moins que t entités peut être identifié par celles-ci.

Une infrastructure à clé publique proactive est une approche visant à contrer les attaques multiples d'adversaires déterminés sur une clé privée ayant une grande durée de vie. Une signature numérique proactive est un type de partage de secret proactif [15]. Un tel partage se déroule en deux phases : une mise à jour périodique et un calcul de fonction. Au départ, un groupe de X entités de confiance se partagent une clé privée, qui correspond à leur clé publique collective, à l'aide du protocole de partage de secret vérifiable (*verifiable secret sharing*) de Feldman. Lors de la mise à jour, le secret est reconstitué puis repartagé entre les X entités selon certains critères. Par conséquent, si un adversaire a accès à une ou plusieurs parts du secret, il doit agir rapidement puisqu'il ne pourra profiter de l'information qu'elle lui procure après la prochaine mise à jour. Les entités calculent ensuite une fonction avec la clé privée partagée (signature numérique, décryptage, etc.) en utilisant chacune leur part. Il a été prouvé que la sécurité de la signature numérique proactive est équivalente à celle du partage de secret proactif qui est sémantiquement sécuritaire (un adversaire avec une puissance de calcul limitée ne peut obtenir d'information sur le message clair à partir du message crypté et des données publiques).

3.4.2 Différences

Pour cette seconde solution, le CAPK est remplacé par le CAC (*Conditionally Anonymous Certificate*) qui procure également à son propriétaire un anonymat révocable. Le CAC, créé par l'autorité de certification sans que celle-ci ne fasse appel au système FOLC ou à un autre système d'argent électronique, certifie une clé publique. L'autorité de certification regroupe ici plusieurs entités et utilise une infrastructure de signature numérique proactive pouvant servir à générer, entre autres, une signature à l'encre magique de manière distribuée. Grâce à cette infrastructure, la signature produite offre une sécurité contre une attaque message clair

choisi et une protection contre la falsification existentielle (*existential forgeability*) : un adversaire ne peut produire une signature valide sur un message en ignorant la clé de signature, qu'il connaisse le contenu du message ou non.

Nous utilisons un nouveau concept, celui de compte anonyme (*anonymous account*). L'investisseur possède un tel compte chez son courtier et le négociateur en détient un à la Bourse; dans ce compte reposent leur argent et leurs actions. Sans l'intervention de l'autorité de certification, l'identité du propriétaire d'un de ces comptes ne peut être connue.

Une action est définie comme étant une donnée numérique ne comportant aucune information sur l'identité de son propriétaire, pouvant être transférée d'un compte anonyme à un autre et portant une signature numérique proactive de la Bourse.

3.4.3 Acteurs

La Bourse est formée de quatre parties distinctes : le SEV (*Stock Exchange Verification*), le SEC (*Stock Exchange Center*), le SEE (*Stock Exchange Election*) et le SET (*Stock Exchange Taxation*). Le SEV reçoit les ordres des négociateurs et vérifie leur contenu en plus d'administrer un babillard anonyme où sont annoncés ces ordres. Le SEC jumelle les ordres, ouvre et gère les comptes anonymes des négociateurs et son propre compte et entretient une base de données des clés publiques des négociateurs enregistrés, accessible qu'à ceux-ci. De plus, il peut retirer un ordre du babillard à la demande d'un négociateur et gère une réserve de certaines actions. Le SEE s'occupe des votes et des dividendes associés à certains titres et le SET, des retenues fiscales.

L'autorité de certification fournit des CAC aux négociateurs et aux investisseurs. Le négociateur, tout comme l'investisseur, joue le même rôle que dans le système de la solution précédente. Le tiers de confiance, quant à lui, n'est plus une entité distincte; il correspond à l'autorité de certification. Le courtier administre une base

de données des clés publiques de ses clients, accessible à ceux-ci, ouvre et gère des comptes anonymes.

3.4.4 Protocoles

L'investisseur et le négociateur accomplissent chacun et une seule fois une procédure d'initialisation. Celle-ci comporte des protocoles d'obtention du CAC et d'ouverture de compte anonyme. D'abord, l'investisseur (le négociateur) fournit sa véritable identité à l'autorité de certification afin d'obtenir un certificat. L'autorité produit alors une signature à l'encre magique proactive sur une clé publique choisie de manière aléatoire par l'investisseur (le négociateur) et associée à une clé privée.

Ensuite, l'investisseur et le négociateur se procurent chacun un compte anonyme, le premier chez son courtier et le second à la Bourse. Plus précisément, ils entreprennent chacun le protocole suivant : l'investisseur (négociateur) produit une signature à l'anneau sur son CAC à l'aide des clés publiques des clients du courtier (des négociateurs enregistrés à la Bourse) et la remet au courtier (au SEC) qui la vérifie. Si la signature et le CAC sont valides, le courtier (le SEC) associe le CAC à un compte choisi au hasard. L'investisseur (le négociateur) peut dorénavant déposer de l'argent, électronique ou non, dans son compte ou en retirer après un protocole d'authentification.

Lorsque l'investisseur souhaite faire une demande d'achat ou de vente, il remet à son courtier une signature numérique de format $sign_s(\textit{type de transaction, compte anonyme, nom de l'action, prix offert ou demandé, nombre d'actions})$ où s est la clé privée associée à la clé publique du CAC correspondant au compte indiqué. Le courtier s'assure en premier que le compte existe. Si tel est le cas, il obtient le CAC associé au compte et vérifie la signature. Ensuite, si la transaction est un achat, il faut que $(\textit{prix offert}) * (\textit{nombre d'actions}) \leq m_{balance}$, où $m_{balance}$ est le solde d'argent dans le compte, pour que la demande soit valide; sinon, il faut que $(\textit{nombre d'actions}) \leq s_{balance}$, où $s_{balance}$ correspond aux actions qui restent dans le compte. Dans tous les cas, si la demande est admissible, le courtier communique avec le

négociateur pour qu'il place un ordre à la Bourse. Le négociateur transmet au SEV une signature numérique de même format que celle produite par l'investisseur et le SEV procède aux mêmes vérifications que le courtier par rapport au compte, à la signature et à son contenu. S'il juge l'ordre valide, le SEV l'annonce sur le babillard.

De façon périodique et à la suite d'une nouvelle annonce sur le babillard, le SEC vérifie si, d'une part, deux ordres peuvent être jumelés ou, d'autre part, si un ordre est au prix courant, si aucun autre ordre ne peut lui être jumelé et s'il maintient une réserve de l'action en question. Si un de ces deux événements se produit, le SEC débite le compte de l'acheteur du montant (*prix offert*) * (*nombre d'actions*) et le compte du vendeur du nombre d'actions approprié. Puis, il transfère les actions dans le compte de l'acheteur et l'argent dans celui du vendeur. Le SET enregistre la transcription de la transaction. Le négociateur communique ensuite à son courtier pour lui faire part de la transaction et pour qu'il transfère, selon le cas, les actions ou l'argent débités de son compte dans le compte de l'investisseur.

Pour retirer une demande, l'investisseur transmet la signature $sign_s$(*retrait, type de transaction, compte anonyme, nom de l'action, prix offert ou demandé, nombre d'actions*) à son courtier qui vérifie la signature et son contenu. Si la signature et les données sont valides, le courtier communique avec le négociateur qui procède exactement de la même façon avec le SEC. Celui-ci retire alors l'ordre du babillard.

3.4.5 Analyse

Fait 3.3. *Les actions électroniques transigées ne sont pas falsifiables et ne peuvent être vendues en double. De plus, la sécurité associée aux actions est équivalente à la sécurité de la signature proactive.*

Justification. Un adversaire ne peut falsifier une action, car il lui faut produire une signature proactive de la Bourse qui est existentiellement infalsifiable. Si la Bourse agit malhonnêtement et émet illégalement une action, cet acte sera décelé :

le chiffre obtenu par l'audit du nombre d'actions dans les comptes anonymes sera différent de celui représentant le nombre d'actions émises légalement. Pour vendre une action en double, il faut placer un ordre de vente valide ce qui signifie détenir l'action dans son compte. Comme l'action a déjà été vendue, il s'agit de la falsifier ou d'empêcher la Bourse de vérifier et de retirer les fonds, ce qui n'est pas possible sans collusion. □

Fait 3.4. *Le système a les propriétés S1 à S7 si nous considérons les deux hypothèses suivantes :*

i. L'autorité de certification – toutes les entités qu'elle regroupe – reste honnête.

ii. Il ne peut y avoir une collusion entre le SEV, le SEC, le SEE et le SET.

Justification. (S1 et S2) Un client (négociateur) est légitime si la signature en anneau qu'il fournit lors de l'ouverture de son compte anonyme est valide. Produire une telle signature sans appartenir au groupe désigné est un problème difficile. Un client (négociateur) est anonyme, parce qu'il choisit un compte au hasard et parce que le CAC lui procure un anonymat calculatoire. (S3) Le SEC et le courtier transfèrent eux-mêmes les données d'un compte anonyme à un autre. La sécurité de la transaction repose donc sur la transcription du protocole et l'audit des transferts de fonds. (S4 et S5) Une signature numérique est requise pour retirer un ordre. Par conséquent, l'entité qui souhaite retirer un ordre dont elle n'est pas l'auteur doit forger une signature. (S6) L'autorité de certification associe toujours un CAC à une véritable identité, car elle est honnête par hypothèse. Pour créer un CAC nullement relié à une identité, il faut forger la signature existentiellement infalsifiable de l'autorité de certification. Le CAC permet de retracer le propriétaire d'un compte anonyme, de retracer le propriétaire d'un CAC et d'associer une identité à un compte et à un CAC. Un compte correspondant à une identité révoquée est gelé. (S7) Le système est sécuritaire contre les attaques suivantes : la recherche exhaustive de la clé de signature de l'autorité de certification, le délit d'initié, le

blanchiment d'argent et l'émission illégale de CAC.

1) Le délit d'initié et le blanchiment d'argent peuvent être détectés par l'analyse des gains et des transcriptions des transactions.
2) Si une entité trouve la clé de l'autorité de certification par une recherche exhaustive et si elle ouvre des comptes associés à aucune identité, cela peut être détecté. Si Σ_{CAC} est le nombre de CAC produits par l'autorité de certification, si $\Sigma_{CAC\,révoqué}$ est le nombre de CAC produits qui ont été révoqués, si Σ_{compte} est le nombre de comptes anonymes existants et si $\Sigma_{CAC} - \Sigma_{CAC\,révoqué} < \Sigma_{compte}$, alors certains CAC ont été falsifiés.
3) Soit $\Sigma_{requête}$ le nombre de requêtes reçues par l'autorité de certification pour des CAC et soit Σ_{CAC} le nombre de CAC produits par l'autorité de certification. Si $\Sigma_{CAC} > \Sigma_{requête}$, l'autorité de certification a émis illégalement des CAC. □

Si nous posons les hypothèses *i* et *ii*, ce système d'échanges boursiers anonymes procure aux entités qui le désirent un anonymat calculatoire et révocable. Si elle le souhaite, une entité peut s'assurer que ses transactions ne peuvent être corrélées.

La sécurité des protocoles dépend du choix de l'infrastructure de signature numérique utilisée par l'investisseur et le négociateur, du choix des infrastructures de signature numérique proactive et de signature à l'encre magique proactive, des transcriptions, des audits et des hypothèses *i* et *ii*.

3.4.6 Remarques

(1) Cette deuxième solution fondée sur le système de MacKenzie et Sorensen est sécuritaire contre un plus grand nombre d'attaques et est plus extensible puisque le nombre d'actions n'influe pas sur la transaction. Une entité peut posséder m CAC et m comptes, pour $m \geq 1$. Lorsque $m = 1$, le système a comme propriété que les transactions d'une même entité ne peuvent être reliées entre elles. Si $m > 1$, ce n'est plus le cas. Cette propriété nuit à l'efficacité et à la possibilité d'extension des protocoles mais ne diminue pas leur sécurité.

(2) Comme le traduisent les hypothèses *i* et *ii*, l'investisseur et le négociateur doivent accorder une confiance totale à l'autorité de certification ainsi qu'à la Bourse. Bien que ces deux parties regroupent ici plus d'une entité, on suppose qu'elles agissent honnêtement. Sans ces hypothèses, l'identité d'une entité anonyme peut être révélée et les actes de la Bourse ne sont plus contrôlés. En effet, un quorum de ces entités peut agir illégalement et irréversiblement. Un quorum des entités formant l'autorité de certification peut révéler l'identité d'un client ou d'un négociateur tandis qu'un quorum des entités à la Bourse peut décider de faire fi des réglementations et des vérifications essentielles au bon fonctionnement du marché boursier – accepter des ordres illégaux ou blanchir de l'argent, par exemple.

(3) Normalement, il n'est pas nécessaire d'avoir les fonds lorsqu'une demande ou un ordre est placé. Ainsi, plusieurs jours sont accordés aux parties concernées pour qu'elles puissent se procurer les fonds nécessaires après l'appariement de leur ordre. Dans ce système, le courtier et le SEV acceptent ou rejettent une demande ou un ordre en fonction des fonds ou des actions se trouvant dans le compte indiqué.

3.5 Troisième solution: notre modèle

Les deux systèmes présentés précédemment modélisent les échanges boursiers anonymes et procurent un anonymat calculatoire révocable à l'aide de certificats. L'investisseur et le négociateur utilisent une clé anonyme certifiée pour communiquer et pour transiger. Dans la solution que nous allons proposer, les certificats sont remplacés par une fonction d'identités substituts : l'entité désirant rester anonyme peut générer elle-même des clés publiques anonymes certifiées. Basé sur les résultats de Christianson et Das Chowdhury [9], ce troisième système d'échange offre un anonymat révocable mais inconditionnel.

3.5.1 Glossaire et définitions

À l'aide d'une fonction d'identités substituts, il est possible de générer des clés publiques pouvant être utilisées comme des identités substituts (*surrogates*), appelées IDS. Dans le cas présent, une personne de confiance distribue et administre les fonctions d'IDS; elle peut ainsi retracer le propriétaire d'une IDS donnée.

Un ordre contient le nom de l'entreprise, le type d'action, le prix offert ou demandé, le type d'ordre (achat ou vente), le nombre d'actions à transiger, un numéro d'identification d'ordre, l'heure et la date, ainsi que l'identité substitut associée à l'ordre. Ces mêmes informations sont indiquées dans une demande. L'investisseur nécessite une IDS pour placer une demande tandis que le négociateur en requiert une pour placer un ordre. L'IDS utilisée est dite valide.

Nous modélisons une action électronique comme une pièce d'argent électronique du FOLC : tandis qu'une telle pièce porte un montant, ce que nous appellerons « jeton » représente plutôt un nombre d'actions d'un certain type. Un tel jeton correspond donc à une ou à plusieurs actions électroniques et se manipule comme de l'argent électronique FOLC : on le retire, on le dépense et on le dépose à l'aide des protocoles de dépôt, de paiement et de retrait du FOLC. De plus, les protocoles de retracement du FOLC conviennent aussi aux jetons; par conséquent, il est possible

de retracer le propriétaire d'une action ainsi qu'une action en particulier.

3.5.2 Acteurs

Le *Trusted Stock Manager*, appelé TSM, est l'acteur que nous ajoutons. Il a le même niveau d'honnêteté et suscite autant la confiance qu'une banque. Il ne fournit aucune information sur ses clients sans raison légitime : une entité doit être dûment authentifiée et identifiée pour que le TSM lui donne une information ou lui rende un service.

Le TSM crée les jetons (les actions) et administre des comptes de titres pour les négociateurs et les investisseurs. Il génère aussi à leur intention une fonction d'identités substituts et gère leurs changements d'identité. Il ajoute des titres en circulation ou les en retire :

- si une entreprise veut mettre de nouveaux titres en circulation, le TSM ajoute ces titres à sa base de données et les cède à la Bourse;
- si une entreprise désire retirer des titres en circulation, le TSM achète ces titres et les élimine de sa base de données.

En plus de la liste de tous les titres en circulation, le TSM garde des listes publiques des IDS valides pour les investisseurs et pour les négociateurs, ainsi que trois listes privées : une pour les IDS d'ordres placés, une seconde pour les IDS d'ordres jumelés et une dernière pour les IDS de demandes jumelées.

La banque gère des comptes bancaires pour ses clients et crée de l'argent électronique FOLC pour ceux qui souhaitent rester anonymes.

Le TSM et la banque ont accès à un tiers de confiance pour les cas où il serait indispensable de retracer une action électronique, de l'argent électronique ou un propriétaire de jeton ou de pièce électronique.

La Bourse tient à jour une liste publique des ordres placés et le courtier, une liste de toutes les demandes n'ayant pas fait l'objet d'une transaction ou d'un retrait.

Pour chaque demande et chaque ordre placés, l'investisseur et le négociateur génèrent une nouvelle IDS. Ainsi, les demandes d'un même investisseur et les ordres d'un même négociateur, c'est-à-dire toutes leurs IDS, ne peuvent être corrélés.

3.5.3 Protocoles

Avant d'effectuer les protocoles, le négociateur et l'investisseur exécutent une procédure d'initialisation qu'ils n'auront pas à répéter. Tout d'abord, ils fournissent leur véritable identité à la banque pour y ouvrir un compte (section 2.3.3). Ensuite, les clients du courtier et les négociateurs qui ont accès au parquet de la Bourse ouvrent un compte de titres au TSM, compte associé à une fonction d'identités substituts et dans lequel seront conservées leurs actions.

Plus précisément, le TSM et l'entité souhaitant ouvrir un compte s'entendent sur P, un grand nombre premier tel qu'il est difficile de trouver un logarithme discret dans le groupe $\mathbb{Z}_P^*$ et tel que $(P-1)$ a un grand facteur premier et aucun petit facteur premier; sinon, trouver un logarithme discret est facile.

1. L'entité envoie au TSM les informations privées nécessaires à la création d'un compte et sa clé publique personnelle $X = g^s$ dans le groupe $\mathbb{Z}_P^*$; g étant générateur de $\mathbb{Z}_P^*$ et $s \in \mathbb{Z}_P^*$.
2. Le TSM vérifie si l'entité est un client du courtier ou un négociateur inscrit à la Bourse et, si c'est le cas, il choisit A, O et σ_0 dans $\mathbb{Z}_P^*$ selon la Méthode de Congruence Linéaire. Plus particulièrement, O et P doivent être premiers entre eux.

   Le TSM envoie alors à l'entité $V = (\sigma_0, O, A)$ et calcule la première identité qu'elle utilisera : $\sigma_1 \equiv (A * \sigma_0 + O) \pmod{P-1}$ et $I_1 \equiv X^{\sigma_1} \pmod{P}$. Il garde en mémoire les informations propres à l'entité, incluant celles qui sont propres à ses identités substituts, $F = (O, A, X, I_1, \sigma_1, P)$, qu'il lie à un compte de titres.

Entité		TSM
	$\xrightarrow{X = g^s}$	
		Choisit σ_0, O, A
	$\xleftarrow{V = (\sigma_0, O, A)}$	
		Calcule σ_1 et I_1
		Archive
		$F = (O, A, X, I_1, \sigma_1, P)$

TAB. 3.7 – *Ouverture d'un compte au TSM*

Protocole de placement d'un ordre

Pour placer la demande i, l'investisseur t calcule son identité substitut I_i :

$$\begin{aligned} \sigma_i &\equiv A * \sigma_{i-1} + O \pmod{P-1} \\ e &\equiv s * \sigma_i \pmod{P-1} \\ I_i &\equiv g^e \pmod{P} \end{aligned}$$

Il produit ensuite une signature en anneau « modifiée » sur la demande qu'il souhaite placer.

1. a. Posons N le nombre de clients du courtier. L'investisseur choisit un groupe de $r \leq N$ identités substituts de clients du courtier qui sont valides et qui contient sa propre identité : $I_1, \ldots, I_r$.
   b. Posons m la description de la demande à placer. L'investisseur utilise la fonction de hachage h, connue par le courtier, sur m pour obtenir k : $k = h(m)$.
   c. L'investisseur choisit aléatoirement $v \in \mathbb{Z}_P^*$.
2. Le courtier choisit indépendamment et uniformément des valeurs $x_1, \ldots, x_r$ (section 2.2.2) et les envoie à l'investisseur.
3. L'investisseur calcule les y_i tel que $y_i = g_i(x_i)$ pour $1 \leq i \leq r, i \neq t$, et résout $F_{k,v}(y_1, \ldots, y_r) = v$ pour y_t, où les g_i et $F_{k,v}(y_1, \ldots, y_r)$ sont des fonctions ayant les propriétés nécessaires énoncées à la section 2.2.2.

4. L'investisseur remet au courtier la signature en anneau produite : $(m; (I_1, \ldots, I_r; v; x_1, \ldots, x_r))$.
5. Le courtier vérifie la signature et obtient I_i. Il envoie I_i au TSM et, à l'investisseur, un numéro de confirmation de la demande placée.

$\mathbf{I_i}$		**Courtier**
Calcule $k = h(m)$		Choisit $(x_1, \ldots, x_r)$
	$\xleftarrow{(x_1, \ldots, x_r)}$	
	$\xrightarrow{(m;\ (I_1, \ldots, I_r;\ v;\ x_1, \ldots, x_r))}$	
		Vérifie $(m;(I_1, \ldots, I_r;\ v;x_1, \ldots, x_r))$ Obtient I_i
	$\xleftarrow{\textit{numéro de confirmation}}$	

TAB. 3.8 – *Placement d'un ordre*

Par après, le courtier communique avec le négociateur qui procède exactement de la même façon avec la Bourse : il calcule sa prochaine IDS et produit aussi une signature en anneau suivant les étapes décrites.

Protocole de synchronisation

Après avoir reçu I_i, le TSM met à jour l'identité substitut de l'investisseur (ou du négociateur) t, c'est-à-dire l'identité que t utilisera à la prochaine transaction. Il calcule donc la prochaine IDS à partir des informations F qu'il avait gardées :

$$\begin{aligned} \sigma_{i+1} &\equiv A * \sigma_i + O \pmod{P-1} \\ e &\equiv s * \sigma_{i+1} \pmod{P-1} \\ I_{i+1} &\equiv g^e \pmod{P} \end{aligned}$$

Dans F, il remplace σ_i et I_i par σ_{i+1} et I_{i+1} respectivement et met à jour la liste publique des IDS valides. Il procède de la même façon pour synchroniser une IDS appartenant à un négociateur.

Protocole de jumelage

Lorsque la Bourse reçoit un nouvel ordre, elle regarde s'il existe un ordre inverse dans sa liste des ordres placés : s'il en existe un, elle jumelle les ordres et communique avec les deux parties intéressées. Sinon, elle vérifie si le prix demandé ou offert est le prix courant de l'action et, si elle possède une réserve de ces actions, elle ne jumelle pas l'ordre en tant que tel mais contacte le négociateur pour effectuer l'échange directement avec lui. Dans tous les cas, le message qu'elle envoie pour annoncer que les ordres sont jumelés ou qu'il peut y avoir échange est un engagement légal pour les parties en cause, Bourse et/ou négociateur(s). Le TSM reçoit les IDS d'ordres d'achat jumelés en vrac à la fin de la journée et transfère à sa liste des IDS jumelées les IDS tirées de sa liste des IDS placées. Le ou les négociateurs ayant transigés informent leur courtier de l'appariement; chaque courtier contacte ensuite l'investisseur approprié.

Protocole d'échange

En un premier temps, l'investisseur effectue un protocole de retrait puis de paiement du FOLC. Il remet ainsi au courtier l'argent électronique correspondant à sa demande ou il transfert le nombre approprié d'actions électroniques au négociateur, par l'intermédiaire du courtier. Le négociateur dépose l'argent qu'il reçoit du courtier ou les actions qu'il a reçues directement de l'investisseur dans son compte bancaire ou de titres, selon le cas.

Investisseur		**Courtier**		**Négociateur**
	paiement de d *dollars* / *ou de* n *actions* ⟷			
			transfert d'argent / *ou d'actions* ⟶	

TAB. 3.9 – *Échange: Première étape*

En un second temps, le vendeur et l'acheteur d'une action – deux négociateurs ou un négociateur et la Bourse – effectuent chacun le protocole de retrait du FOLC pour obtenir respectivement un jeton correspondant aux actions électroniques et

une pièce d'argent électronique et exécutent ensuite le protocole de paiement du FOLC pour transiger actions et argent. L'acheteur dépose les actions reçues dans son compte au TSM : il accomplit le protocole de dépôt du FOLC et fournit l'IDS et le numéro de confirmation correspondant à l'ordre au TSM. Le vendeur dépose l'argent reçu à la banque. Après la transaction, chaque négociateur contacte son courtier qui transmet au TSM, en vrac, à la fin de la journée, les IDS associées aux demandes d'achat jumelées.

Acheteur		**Vendeur**
	paiement de d *dollars* $\longleftrightarrow$	
	paiement de n *actions* $\longleftrightarrow$	

TAB. 3.10 – *Échange: Deuxième étape*

Finalement, dans le cas d'une vente, le négociateur transfert de manière non électronique l'argent provenant de la transaction au courtier, lequel réalise ensuite un protocole retrait puis de paiement pour remettre l'argent à l'investisseur. Ce dernier dépose alors les fonds dans son compte bancaire. Dans le cas d'un achat, le négociateur effectue un protocole de retrait puis de paiement avec l'investisseur par l'intermédiaire du courtier. L'investisseur dépose ensuite ses actions dans son compte au TSM en lui fournissant l'IDS et le numéro de confirmation correspondant à la demande.

Investisseur	**Courtier**	**Négociateur**
Vente:		*transfert d'argent* $\longleftarrow$
	paiement de d *dollars* $\longleftarrow$	
Achat:		*paiement de* n *actions* $\longleftarrow$
	paiement de n *actions* $\longleftarrow$	

TAB. 3.11 – *Échange: Troisième étape*

Protocole de retrait d'un ordre

Si un investisseur souhaite retirer sa demande d'achat ou de vente, il transmet au courtier un message, contenant la date et l'heure, signé avec la clé privée associée à l'IDS de la demande en question. Si la signature est valide, le courtier fournit un numéro de confirmation à l'investisseur, demande au négociateur de procéder au retrait de l'ordre correspondant à la Bourse et retire cette demande de la liste. Le négociateur procède de la même façon avec la Bourse. Celle-ci élimine l'ordre de sa liste et avise le TSM du retrait en lui fournissant l'IDS correspondante. Le TSM retire cette IDS de ses listes.

3.5.4 Analyse

Fait 3.5. *Modélisés exactement comme les pièces électroniques du FOLC, les jetons – les actions électroniques – possèdent les mêmes propriétés de sécurité que les pièces. En particulier, ils ne sont pas falsifiables, ne peuvent être vendus en double et seule la Bourse peut les créer.*

Fait 3.6. *Notre système possède les propriétés de sécurité S1 à S7.*

Justification. Les actions assurent aux utilisateurs un anonymat calculatoire grâce aux propriétés P1 et P8 du FOLC. Un adversaire réussirait à placer un ordre ou une demande s'il produisait une signature en anneau valide : la signature à fournir ne devrait pas comporter une IDS qui ne figure pas sur la liste publique des IDS valides et elle devrait être acceptée après vérification. Comme l'appartenance au groupe auquel l'adversaire s'identifierait pour générer la signature en anneau est calculatoire, il lui faudrait résoudre un problème difficile pour produire une signature valide.

L'anonymat du client et du négociateur peut facilement être révoqué. On peut efficacement retracer le propriétaire d'un jeton ou d'une pièce électronique puisque

leur anonymat est contrôlé (propriétés P2 et P4). De plus, le courtier et le TSM gardent chacun une liste des IDS placées ainsi que la fonction d'IDS de chacun de leurs clients. Ainsi, ils peuvent facilement retracer l'auteur d'une demande ou d'un ordre. La Bourse ne peut pas placer légitimement des ordres sous une autre identité, car le TSM ne lui accorde pas une fonction d'IDS. Pour agir malhonnêtement, elle doit utiliser une IDS appartenant à un négociateur (*impersonation*) et résoudre, comme tout autre adversaire, des problèmes difficiles pour réussir ce qu'elle veut entreprendre; ceci peut être néanmoins détecté par le négociateur dont l'identité a été usurpée.

Comme l'investisseur et le négociateur génèrent une nouvelle IDS pour chaque demande et chaque ordre placés, les demandes d'un même investisseur et les ordres d'un même négociateur, c'est-à-dire toutes leurs IDS, ne peuvent être corrélés.

Les actions sont sécuritaires face à toutes les entités malhonnêtes puisqu'elles ont la propriété P7. De plus, la Bourse ne peut pas oublier de synchroniser une IDS ou de retirer un ordre, les listes des ordres placés et des IDS valides étant publiques. Un audit des transactions, des placements d'ordres et de demandes permettrait de découvrir toute collusion entre la Bourse, le négociateur, le courtier et l'investisseur.

Une fois que la Bourse envoie le message confirmant l'appariement des ordres, qui obligera les deux parties concernées à transiger, un adversaire doit utiliser une IDS ne lui appartenant pas pour effectuer les protocoles de paiement et de dépôt. Pour réussir à transiger et à déposer correctement, il lui faudra résoudre au moins un problème difficile, tel que Logarithme discret. Pour retirer un ordre ou une demande, il lui faut produire une signature numérique valide associée à une certaine IDS qui n'est pas la sienne. La sécurité du protocole de retrait d'un ordre est calculatoire et dépend de l'infrastructure de signature numérique utilisée. □

Sécurité calculatoire, anonymat inconditionnel : preuves

Supposons qu'il est possible de trouver un logarithme discret dans le groupe $\mathbb{Z}_P^*$ à l'aide d'un algorithme efficace. Supposons que nous détenons trois IDS de suite, d'une même identité, c'est-à-dire $I_n \equiv g^{s*\sigma_n} \pmod{P}$, $I_{n+1} \equiv g^{s*\sigma_{n+1}} \pmod{P}$ et $I_{n+2} \equiv g^{s*\sigma_{n+2}} \pmod{P}$, avec $n \geq 1$. Après avoir exécuté l'algorithme à trois reprises, nous obtenons ces trois logarithmes discrets : $s * \sigma_n \pmod{P-1}$, $s * \sigma_{n+1} \pmod{P-1}$ et $s * \sigma_{n+2} \pmod{P-1}$.

Fait 3.7. *Alors, nous pouvons prédire la prochaine IDS, c'est-à-dire calculer le prochain exposant* $s * \sigma_{n+3} \pmod{P-1}$, *de même que toutes les IDS suivantes.*

Justification. Posons

(i) $y_n \equiv s * \sigma_n \pmod{P-1}$

(ii) $y_{n+1} \equiv s * \sigma_{n+1} \equiv s * (A * \sigma_n + O) \equiv A * y_n + s * O \pmod{P-1}$

(iii) $y_{n+2} \equiv s * \sigma_{n+2} \equiv s * (A * \sigma_{n+1} + O) \equiv A * y_{n+1} + s * O \pmod{P-1}$

(iv) $y_{n+2} - y_{n+1} \equiv A * y_{n+1} - A * y_n \equiv A * (y_{n+1} - y_n) \pmod{P-1}$

Ayant y_n, y_{n+1} et y_{n+2} déjà en main, nous trouvons A à l'aide de (iv).

(v) $y_{n+1} - y_n \equiv y_{n+1} - A * y_n \equiv s * O$

Ayant y_n, y_{n+1} et A déjà en main, nous trouvons $s * O$ à l'aide de (v). À partir de y_{n+2} , A et $s * O$, nous pouvons générer $y_{n+3} \equiv s * \sigma_{n+3} \equiv s * (A * \sigma_{n+2} + O) \equiv A * y_{n+3} + s * O \pmod{P-1}$ et les IDS suivantes. □

Fait 3.8. *Nous pouvons aussi trouver les IDS précédant* I_n*; en particulier, nous pouvons trouver* $s * \sigma_{n-1} \pmod{P-1}$.

Justification. Nous avons y_n en main et nous avons trouvé A et $s * O$. Puisque $y_n \equiv s * \sigma_n \equiv s * (A * \sigma_{n-1} + O) \equiv A * y_{n-1} + s * O$, alors $y_{n-1} \equiv (y_n - (s * O)) * (A)^{-1}$ et ainsi de suite pour $y_{n-2}, \ldots, y_1$. □

Fait 3.9. *La sécurité de la valeur s est inconditionnelle.*

En particulier, même si l'on peut résoudre efficacement le problème Logarithme discret pour le groupe $\mathbb{Z}_P^*$, la valeur s reste inconditionnellement cachée.

Justification. Un adversaire à l'écoute a le système d'équations suivant :

$s * \sigma_1 \equiv A * (s * \sigma_0) + s * O \pmod{P-1}$

$s * \sigma_2 \equiv A * (s * \sigma_1) + s * O \pmod{P-1}$

$\vdots$

$s * \sigma_{P-1} \equiv A * (s * \sigma_{P-2}) + s * O \pmod{P-1}$

En ayant les valeurs A, $s * O$ et $s * \sigma_i$, nous ne pouvons pas résoudre le système d'équations pour s, car s peut prendre toutes les valeurs dans $\mathbb{Z}_P^*$. □

Considérons maintenant que le groupe multiplicatif utilisé est $\mathcal{G}$, groupe cyclique dans lequel il est difficile de trouver un logarithme discret, dont l'ordre est $|\mathcal{G}|$. Nous posons g et h des générateurs du groupe $\mathcal{G}$ tels que $h = g^s$, s une valeur secrète. Nous voulons prouver qu'il n'existe pas un algorithme générique efficace qui résout le problème suivant :

Problème : trouver h^{σ_i} à partir de h^{σ_1}, ..., $h^{\sigma_{i-1}}$ étant donné que

1) h est inconnu et que
2) $\sigma_1 \equiv (A * \sigma_0 + O) \pmod{|\mathcal{G}|}$ et $\sigma_j \equiv (A * \sigma_{j-1} + O) \pmod{|\mathcal{G}|}$ pour A, O et σ_0 inconnus dans $\mathcal{G}$.

Dans l'énoncé et la preuve du prochain théorème, la notation $O(\cdot)$ sera utilisée pour désigner l'ordre d'une fonction; ne pas confondre avec la variable O définie dans le problème.

Théorème 3.4. *Pour le problème énoncé ci-dessus, s'il existe un algorithme générique procédant en T étapes, la probabilité qu'il génère h^{σ_i} est de l'ordre de $\frac{T^2}{Q}$, où Q est le plus grand facteur divisant $|\mathcal{G}|$.*

Démonstration. Soient $h^{A*\sigma_0+O}, \ldots, h^{A^{i-1}*\sigma_0+\ldots+O}$ les éléments au départ. Posons

$P_1 = \sigma_1 \equiv A * \sigma_0 + O$

$\vdots$

$P_{i-1} = \sigma_{i-1} \equiv A^{i-1} * \sigma_0 + \ldots + O$

où les $P_j(A)$, $1 \leq j \leq i-1$, sont des polynômes de variable A et de degré plus petit ou égal à $i-1$, avec σ_0 et O inconnus. Nous cherchons $h^{\sigma_i} = h^{P_i(A)} = h^{A^{i-1}*\sigma_0+\ldots+O}$.

Par ses propriétés, l'algorithme générique ne peut que faire l'opération du groupe, c'est-à-dire multiplier deux éléments dans le groupe. Après l'exécution de l'algorithme, c'est-à-dire après T étapes, nous détenons $(i-1)+T$ éléments de degré plus petit ou égal à $i-1$, car $h^{P_k(A)} * h^{P_l(A)} = h^{P_m(A)}$ où $P_m(A) = P_k(A) + P_l(A)$ et $P_m(A)$ est de degré plus petit ou égal à $i-1$.

L'algorithme générique réussit lorsqu'il trouve $h^{P_i(A)}$, c'est-à-dire si l'un des deux événements suivants se produit :

E1 : au moins deux des $(i-1)+T$ éléments sont égaux.

E2 : un des $(i-1)+T$ éléments est en fait $h^{P_i(A)}$.

Pour que **E1** se produise, il faut que $P_j(A) = P_{j'}(A)$ pour $j \neq j'$, $1 \leq j \leq i-1+T$ et $1 \leq j' \leq i-1+T$. Posons $\mathbf{P}(A) = P_j(A)$ et $\underline{\mathbf{P}}(A) = (P_j - P_{j'})(A) = 0$. Le lemme 9.2 de [27] énonce que la probabilité que $\mathbf{P}(A) = \underline{\mathbf{P}}(A)$ pour un certain j et j' est plus petite ou égale à $\frac{i-1}{Q}$. Alors, la probabilité qu'il existe j et j' tels que $\mathbf{P}(A) = \underline{\mathbf{P}}(A)$, c'est-à-dire la probabilité que **E1** se produise, est

$$\begin{aligned}
\text{Prob}(\mathbf{E1}) &\leq \frac{i-1}{Q}\binom{i-1+T}{2} \\
&= \frac{i-1}{Q}\frac{(i-1+T)!}{2!\,(i-3+T)!} \\
&= \frac{i-1}{Q}(i-1+T)(i-2+T) \\
\text{Prob}(\mathbf{E1}) &= O(\frac{T^2}{Q})
\end{aligned}$$

E2 a lieu si $P_j(A) = \mathbf{P}'(A)$ pour $\mathbf{P}'(A) = \sigma_i = A^{i-1} * \sigma_0 + ... + O$ et $1 \leq j \leq i - 1 + T$. En posant $\mathbf{P}''(A) = (P_j - \mathbf{P}')(A) = 0$, nous avons, d'après le même lemme, que la probabilité que $P_j(A) = \mathbf{P}''(A)$ pour un certain j est plus petite ou égale à $\frac{i}{Q}$. Donc, Prob(**E2**) $\leq (\frac{i}{Q})(i-1+T)$, c'est-à-dire Prob(**E2**)$= O(\frac{T}{Q})$.

La probabilité de succès de l'algorithme, α, est certainement plus petite ou égale à la somme des probabilités de **E1** et **E2**. Donc, $\alpha = O(\frac{T^2}{Q})$.

Pour un algorithme générique exécutant T étapes, on a donc que la probabilité de succès, notée α, est de l'ordre de $\frac{T^2}{Q}$. Cela signifie que $\exists\, c > 0$ et $T_0 > 0$ deux constantes telles que $0 \leq \alpha \leq \frac{cT^2}{Q}$, $\forall T \geq T_0$.
Pour une probabilité de succès fixe α, un algorithme doit procéder en $k\sqrt{\alpha Q}$ étapes ou plus pour $k = \sqrt{1/c}$, si $k\sqrt{\alpha Q} \geq T_0$. Ainsi, $T = \Omega(\sqrt{Q})$.

En utilisant le groupe $\mathbb{Z}_P^*$, cela signifie que pour un algorithme générique exécutant T étapes, la probabilité de succès, notée α, est de l'ordre de $\frac{T^2}{P}$. Cela signifie que $\exists\, c > 0$ et $T_0 > 0$ deux constantes telles que $0 \leq \alpha \leq \frac{cT^2}{P}$, $\forall T \geq T_0$.
Pour une probabilité de succès fixe α, un algorithme doit procéder en $k\sqrt{\alpha P}$ étapes ou plus pour $k = \sqrt{1/c}$, si $k\sqrt{\alpha P} \geq T_0$. Ainsi, $T = \Omega(\sqrt{P})$. □

Générer une IDS sans information équivaut à trouver un logarithme discret dans $\mathbb{Z}_P^*$ ou à trouver un algorithme générique avec une probabilité maximale de réussite de $O(\frac{T^2}{P})$ en $\Omega(\sqrt{P})$ étapes ou plus. Relier une IDS d'une certaine fonction à une autre IDS de la même fonction équivaut à résoudre le problème Logarithme discret. En somme, les IDS procurent un anonymat inconditionnel à leur utilisateur bien que l'argent et les actions électroniques utilisés procurent, par définition, un anonymat calculatoire, car si un adversaire obtient une identité liée à un jeton ou une pièce électronique, il obtient une IDS.

	Première solution	Deuxième solution	Troisième solution
Basé sur l'article de	MacKenzie et Sorensen [19]	Xu, Yung et Zhang [18]	Christianson et Das Chowdhury [9]
Type d'anonymat	Calculatoire et révocable	Calculatoire et révocable	Inconditionnel et révocable
Authentification	Signature en anneau fournie pour placer un ordre ou une demande.	Véritable identité fournie pour recevoir un CAC. Signature en anneau fournie pour ouvrir un compte anonyme.	Véritable identité fournie pour recevoir une fonction d'identités substituts. Signature en anneau fournie pour placer un ordre ou une demande.
Possibilité de relier les transactions d'une entité entre elles	Les transactions ne peuvent être corrélées si une entité se procure un nouveau CAPK pour chaque transaction (inconditionnellement). Une seule action peut être transigée à la fois.	Les transactions ne peuvent être corrélées si une entité se procure un nouveau CAC et un nouveau compte anonyme pour chaque transaction (inconditionnellement). Une ou plusieurs actions peuvent être transigées à la fois.	Les transactions ne peuvent être corrélées (calculatoire). Une ou plusieurs actions peuvent être transigées à la fois à l'aide d'un seul jeton.
Définition d'une action	Une action est un CAPK signé par la Bourse.	Une action est une donnée numérique comportant une signature proactive de la Bourse.	Un jeton est construit comme une pièce du FOLC et représente une ou plusieurs actions.
Système d'argent électronique	FOLC	Au choix	FOLC
Adversaires	Le tiers de confiance et l'autorité de certification sont honnêtes.	L'autorité de certification – toutes les entités qu'elle regroupe – reste honnête et il ne peut y avoir collusion entre les quatre parties formant la Bourse.	Seuls le TSM et la banque sont honnêtes.
Sécurité basée sur	– les propriétés du CAPK – les propriétés du FOLC – le choix de l'infrastructure de signature numérique	– les infrastructures de signature numérique proactive et de signature à l'encre magique – les hypothèses posées	– les propriétés du FOLC – le problème Logarithme discret

TAB. 3.12 – *Comparaison entre les trois systèmes d'échanges anonymes pour la Bourse*

Discussion et conclusion

Consciemment ou non, nous diffusons nos renseignements personnels sur Internet. Les entreprises et organisations avec lesquelles nous faisons affaires analysent l'ensemble des renseignements personnels qu'elles ont pu recueillir et peuvent ainsi déceler les tendances et monter des dossiers afin d'ajuster leur plan marketing. Nous n'avons malheureusement aucun contrôle sur l'utilisation des renseignements que nous fournissons et, plus souvent qu'autrement, les conséquences ne nous sont pas favorables. Cet état de fait incite un nombre croissant d'utilisateurs à demeurer anonymes en ayant recours à des pseudonymes quand l'identité est requise. Employer le même pseudonyme à plusieurs reprises permet cependant d'associer différentes opérations à une même entité. Selon la méthode d'exploration de données (*data mining*) choisie, l'identité, même si elle reste secrète, peut parfois être révélée par une analyse multidimensionnelle. Par conséquent, certains cherchent à s'assurer que leurs opérations ne puissent être reliées entre elles. Ainsi, ils ne jouent pas un rôle actif dans la divulgation de leur identité.

Nous avons analysé les systèmes d'actions électroniques existants et nous avons expliqué pourquoi ils sont plus ou moins appropriés pour les échanges boursiers. Ensuite, nous avons défini le problème et créé, en guise de solution, trois systèmes

d'échange d'actions pour la Bourse qui offrent la possibilité de rester anonyme, fournissent un niveau de sécurité convenable et font en sorte que les diverses transactions d'un même investisseur ou d'un même négociateur ne peuvent être corrélées.

La première de ces solutions est basée sur un modèle sécuritaire. Cependant, compte tenu du nombre de transactions effectuées à la Bourse en une journée, les protocoles que nous avons conçus ne sont pas des plus extensibles. Par exemple, la Bourse doit générer une signature pour chaque action transigée et une seule action peut être transigée à la fois. De plus, pour éviter que ses transactions puissent être reliées entre elles, l'entité doit se procurer une clé publique distincte pour chaque action qu'elle possède.

Notre seconde solution propose donc un système extensible : le nombre d'actions par transaction varie et la Bourse génère une seule signature par action, au moment où elle la crée. De plus, pour que les opérations d'une même entité ne puissent être associées, il est nécessaire de se procurer une clé publique pour chaque transaction, et non pour chaque action. Contrairement au système précédent, il faut faire davantage confiance à l'autorité de certification et à la Bourse, car elles sont toutes deux des entités distribuées devant rester honnêtes en tout temps.

Par conséquent, nous croyons que notre système, qui constitue la troisième solution, est encore plus efficace et plus extensible. De plus, la Bourse peut être considérée comme étant un adversaire et il n'est pas nécessaire que les fonds soient disponibles avant la transaction. Ce système est en outre supérieur puisqu'il offre un anonymat inconditionnel et qu'il n'existe pas d'algorithme générique efficace permettant de prévoir une identité substitut, c'est-à-dire de corréler les diverses transactions d'une même entité. Notre système possède une autre caractéristique importante : nous adaptons les protocoles d'un système d'argent électronique à un système d'actions électroniques. Ainsi, une amélioration du système d'argent électronique engendre une amélioration de notre système d'actions et vice versa.

Autres applications de notre modèle

Pour appliquer notre modèle aux deux autres modes d'échange d'actions, il faut légèrement adapter certains protocoles. La définition technique d'une action demeure néanmoins la même : c'est un jeton qu'il faut retirer ou déposer avec l'aide d'une entité honnête et qui possède les mêmes propriétés qu'une pièce d'argent électronique FOLC. Ainsi, pour le marché hors cote, les protocoles peuvent être modifiés pour qu'un serveur remplace la Bourse et qu'il intervienne lors de l'échange. Par contre, bien que le concept de jeton et le protocole d'échange soient adéquats pour les échanges sur le marché institutionnel, l'anonymat n'est pas justifié dans ce contexte. Lorsque de gros volumes d'actions sont transigés, les identités des deux parties intéressées doivent être connues (par après, surtout) de tous les participants à la Bourse (actionnaires, négociateurs, courtiers, etc.).

Nos protocoles de placement, retrait et jumelage d'un ordre peuvent être employés pour transiger d'autres types de produits financiers tels que les obligations, les titres à valeur fixe et les produits dérivés. De plus, il est possible d'utiliser les fonctions d'identités substituts dans d'autres contextes, par exemple, les enchères électroniques et les communications anonymes ainsi que les transactions bancaires et commerciales.

Possibilités d'amélioration de l'efficacité et de la sécurité: problèmes ouverts

L'efficacité de nos protocoles dépend principalement du groupe choisi, des protocoles du FOLC et de la rapidité avec laquelle il est possible d'apparier deux ordres. Présentement, les méthodes qui permettent de calculer un logarithme discret sur une courbe elliptique sont beaucoup moins efficaces que celles permettant de calculer un logarithme discret dans les groupes conventionnels. De plus, on

croit généralement que le problème Logarithme discret sur les courbes elliptiques est plus difficile, bien que les clés employées soient plus courtes et que la sécurité soit équivalente. Pour ces raisons, et parce que le théorème 4.7 restera valide, nous pouvons utiliser une courbe elliptique au lieu de $\mathbb{Z}_p^*$ comme groupe, pour les protocoles de notre modèle.

À condition que sa définition d'une pièce d'argent électronique convienne aussi pour une action électronique, un système d'argent électronique plus efficace que FOLC améliorerait sans aucun doute notre système d'actions électroniques. En particulier, nous pourrions définir autrement les actions électroniques sans modifier l'utilité des fonctions d'identités substituts.

Le protocole de jumelage est au centre des échanges boursiers, car la rapidité d'appariement influence le nombre de transactions pouvant être effectuées en une journée. Il faut donc porter une attention particulière à l'efficacité lors du choix de l'algorithme d'appariement.

La sécurité des protocoles de notre modèle dépend, entre autres, de la sécurité des signatures numériques que nous avons choisies. Pour implémenter le protocole d'échange, nous pouvons utiliser la méthode appelée *signcryption*. Celle-ci est efficace, car elle permet de crypter et de signer un message en même temps. Trouver le texte clair une fois qu'il a été « crypté-signé » et forger un tel «cryptage-signature » sans connaître la clé privée utilisée nécessitent la résolution d'un problème jugé difficile.

La signature en anneau que nous utilisons lors du placement d'une demande ou d'un ordre pourrait être remplacée par une autre méthode d'authentification ou un autre type de signature en anneau. En effet, la signature en anneau basée sur l'identité (*identity-based ring signature*) et la signature en anneau mandataire (*proxy ring signature*) sont appropriées dans ce contexte. La première signature nécessite une clé publique générée à l'aide de l'identité du membre du groupe et la seconde permet à plusieurs entités d'endosser la responsabilité d'investissement : le

signataire original désigne un ou plusieurs mandataires pouvant signer en son nom. Ces deux signatures en anneau fournissent, elles aussi, un anonymat inconditionnel et en forger une revient à résoudre un problème difficile. Il également est possible d'utiliser les courbes elliptiques pour générer ces deux types de signature en anneau. Comme chaque placement d'ordre ou de demande exige une signature en anneau, le recours à l'une ou l'autre de ces signatures augmente l'efficacité de notre système.

Bibliographie

[1] A. Beimel et S. Dolev. Buses for Anonymous Message Delivery. *Journal of Cryptology*, 16(1): 25-39, 2003.

[2] Z. Bodie, A. Kane, A. Marcus, S. Perrakis et P. Ryan. *Investments.* McGraw-Hill Ryerson, 2003.

[3] Stefan Brands. Untraceable Off-line Cash in Wallets with Observers. Dans *Advances in Cryptology: Proceedings of Crypto '93*, volume 773 de *Lecture Notes in Computer Science*, pages 302-318. Springer-Verlag, 1994.

[4] Gilles Brassard. *Cryptologie contemporaine.* Masson, 1993.

[5] David Chaum. Blind Signatures for Untraceable Payments. Dans *Advances in Cryptology : Proceedings of Crypto '82*, pages 199-203, 1983.

[6] D. Chaum, A. Fiat et M. Naor. Untraceable Electronic Cash. Dans *Advances in Cryptology: Proceedings of Crypto '88*, volume 403 de *Lecture Notes in Computer Science*, pages 319-327. Springer-Verlag, 1990.

[7] David Chaum. Zero-Knowledge Undeniable Signatures. Dans *Advances in Cryptology: Proceedings of Eurocrypt '90*, volume 473 de *Lecture Notes in Computer Science*, pages 458-464. Springer-Verlag, 1991.

[8] D. Chaum et E. van Heyst. Group Signatures. Dans *Advances in Cryptology: Proceedings of Eurocrypt '91*, volume 547 de *Lecture Notes in Computer Science*, pages 302-318. Springer-Verlag, 1991.

[9] P. Das Chowdhury et B. Christianson. Uncorreletable Electronic Transactions using Ring Signatures. *SICS/Wholes Conference*, 2004.

[10] Giovanni Di Crescenzo. Privacy for the Stock Market. Dans *Financial Cryptography: Proceedings of the Fifth International Conference*, volume 2339 de

Lecture Notes in Computer Science, pages 269-288. Springer, 2002.

[11] G. Davida, A. Fiat, Y. Tsiounis et M. Yung. Anonymity Control in E-Cash Systems. Dans *Financial Cryptography: Proceedings of the First International Conference*, volume 1318 de *Lecture Notes in Computer Science*, pages 1-16. Springer, 1997.

[12] Y. Frankel, Y. Tsiounis et M. Yung. Indirect Discourse Proofs: Achieving Efficient Fair Off-line E-Cash. Dans *Advances in Cryptology: Proceedings of Asiacrypt '96*, volume 1163 de *Lecture Notes in Computer Science*, pages 286-300. Springer, 1996.

[13] Y. Frankel, Y. Tsiounis et M. Yung. Fair Off-line E-Cash Made Easy. Dans *Advances in Cryptology: Proceedings of Asiacrypt '98*, volume 1514 de *Lecture Notes in Computer Science*, pages 257-270. Springer, 1998.

[14] M. Franklin et M. Yung. Secure and Efficient Off-line Digital Money. *ICALP: Automata, Languages and Programming*, volume 700 de *Lecture Notes in Computer Science*, pages 265-276. Springer-Verlag, 1993.

[15] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk et M. Yung. Proactive Public Key and Signature Systems. Dans *4th ACM Conference on Computer and Communications Security*, pages 100-110, 1997.

[16] M. Jakobsson et M. Yung. Distributed "Magic Ink" Signatures. Dans *Advances in Cryptology: Proceedings of Eurocrypt '97*, volume 1233 de *Lecture Notes in Computer Science*, pages 450-464. Springer, 1997.

[17] Donald E. Knut. *The Art of Computer Programming.* Volume 2, Addison-Wesley, 1971.

[18] S. Ku, M. Yung et G. Zhang. Scalable, Tax-Evasion Free, Anonymous Investing. Dans *IFIP/SEC 2000: Fifteenth International Conference on Information Security*, 2000.

[19] P. Mackenzie. et J. Sorensen. Anonymous Investing: Hiding the Identities of Stockholders. Dans *Financial Cryptography: Proceedings of the Third International Conference*, volume 1648 de *Lecture Notes in Computer Science*, pages 212-229. Springer, 1999.

[20] S. Matsuo et W. Ogata. A Method for Exchanging Valuable Data: How to Realize Matching Oblivious Transfer. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, E86-A(1): 189-203, Janvier 2003.

[21] A. Menezes, P. van Oorschot et S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 2001.

[22] K. Oishi, M. Mambo et E. Okamoto. Anonymous Public Key Certificates and Their Applications. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E81-A(1): 56-64, Janvier 1998.

[23] Ronald Rivest. Can We Eliminate Certificate Revocation Lists? Dans *Financial Cryptography: Proceedings of the Second International Conference*, volume 1465 de *Lecture Notes in Computer Science*, pages 178-183. Springer, 1998.

[24] R. Rivest, A. Shamir et Y. Tauman. How to Leak a Secret. Dans *Advances in Cryptology: Proceedings of Asiacrypt '01*, volume 2248 de *Lecture Notes in Computer Science*, pages 552-565. Springer, 2001.

[25] S. Schechter, T. Parnell et A. Hartemink. Anonymous Authentication of Membership in Dynamic Groups. Dans *Financial Cryptography: Proceedings of the Third International Conference*, volume 1648 de *Lecture Notes in Computer Science*, pages 184-195. Springer, 1999.

[26] C. Shields et B. N. Levine. A Protocol for Anonymous Communication Over the Internet. Dans *7th ACM Conference on Computer and Communications Security*, pages 33-42, 2000.

[27] V. Shoup. Lower bounds for discrete logarithms and related problems. Dans *Advances in Cryptology: Proceedings of Eurocrypt '97*, volume 1233 de *Lecture Notes in Computer Science*, pages 256-266. Springer, 1997.

[28] S. von Solms et D. Naccache. On Blind Signatures and Perfect Crimes. *Computer and Security*, (11)6 : 581-583, 1992.

[29] M. Stadler, J.M. Piveteau et J. Camenisch. Fair Blind Signatures. Dans *Advances in Cryptology: Proceedings of Eurocrypt '95*, volume 921 de *Lecture Notes in Computer Science*, pages 209-219. Springer, 1995.

[30] Douglas Stinson. *Cryptography : Theory and Practice.* Chapman & Hall/CRC, 2002.

[31] Yiannis Tsiounis. Efficient Electronic Cash: New Notions and Techniques. Thèse de doctorat. Département d'informatique, Northeastern University, 1997.