Stratégies & Information

Stratégies économiques◊ Cognitique financière◊ Gestion de risques◊ Marchés

EDITORIAL

La finance et la banque moderne ne peuvent plus ignorer la cryptologie. Cette technique, dont on pouvait à peine parler en France il y a une quarantaine d'années, sous peine d'encourir les foudres de l'État, est devenue si prégnante que le financier ne peut plus se permettre d'en ignorer à tout le moins les bases. Blockchains, monnaies virtuelles, notarisation répartie et ainsi de suite deviennent des mots que l'on retrouve dans toutes les revues financières. La base en est la cryptologie. Ceci explique que vous trouverez dans ce numéro et dans le prochain deux articles de fond qui sont une introduction à la cryptologie.

Joël Lebidois a été et est l'un des grands spécialistes en France de la cryptologie avant de devenir un spécialiste de la finance (il est en particulier l'auteur de l'ouvrage « Finances pour les ingénieurs » Ed .Maxima Paris 2013).

La titrisation au secours du crédit

Andrea Brignone

La titrisation est un outil souvent mal connu même des milieux financiers et ce d'autant plus que la crise des subprimes a fait porter à ce mécanisme la responsabilité de celle-ci sans voir qu'en réalité la responsabilité n'en incombait pas à la titrisation elle même mais au comportement de certaines banques et surtout du gouvernement américain, qui pour des raisons politiques en avait supprimé les gardes fous. En ce qui concerne les pays européens, les taux de défaut ont été très faibles.

Dans ce petit article, nous essayerons de donner les principes de la titrisation, son intérêt et ses risques. Il s'agit ici seulement d'un survol car la titrisation est un mécanisme complexe faisant intervenir de nombreux acteurs et nécessitant une série de techniques financières complexes. (Suite page 7)

La cryptologie au quotidien

Joël Lebidois

Face aux menaces pesant sur la sécurité nationale,
notre économie et nos concitoyens,
la France a fait de la sécurité du numérique
une priorité stratégique[1]

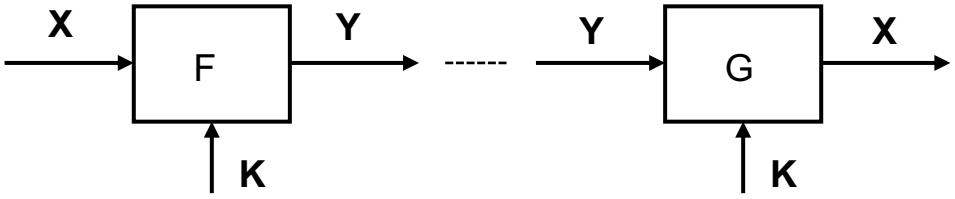
Au premier rang des indispensables outils de protection de l'information figurent les moyens de cryptographie, qui permettent d'assurer le niveau de sécurité requis lors de la transmission, du stockage et de l'accès aux données numériques sensibles. L'usage de ces moyens de cryptographie, auparavant très encadré réglementairement, tend à se généraliser. Le développement et la diffusion de solutions de sécurité robustes et de confiance est encouragé. (suite page 2)

. La législation française donne explicitement la liberté d'usage de ces moyens, en recherchant un juste équilibre entre la protection des libertés individuelles et la sécurité collective. Au plan théorique, ces moyens font appel à la cryptologie qui fut longtemps confinée à la seule science du secret, mais qui est aujourd'hui une science à part entière s'appuyant sur la théorie des nombres, l'algèbre, la théorie de l'information et celle de la complexité. Cette cryptologie moderne s'est développée au même rythme que celui de la numérisation de l'information qui se confond elle-même avec la numérisation de notre société. Certes, pendant longtemps, la cryptologie a surtout été appliquée aux systèmes de chiffrement de l'information c'est-à-dire à la cryptographie ; mais la nécessité de reconstituer la notion de signature ou d'authenticité ou d'intégrité dans le cadre d'une dématérialisation généralisée des textes et des transactions, a conduit à un élargissement considérable du champ de la cryptologie, bien au-delà du seul chiffrement ; au point que, bien souvent à notre insu, la cryptographie se démocratise et pénètre petit à petit notre vie quotidienne.

Première partie : notions et mécanismes de base

Système de chiffrement symétrique

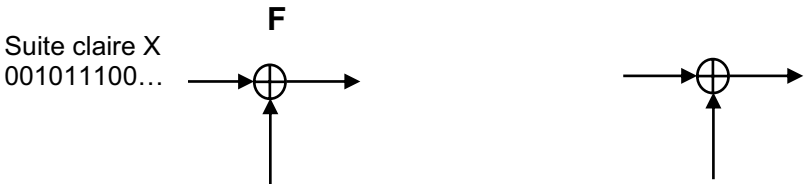
Très généralement, un texte clair, *X*, est transformé en un texte chiffré ou cryptogramme, *Y*, grâce à un algorithme de chiffrement, *F*, qui dépend lui-même d'une clé *K* qui agit comme un paramètre du système.



Cet algorithme *F* possède impérativement un algorithme inverse, *G*, qui permet le déchiffrement avec la même clé *K*. Ainsi :

$$Y = F(K, X) \quad et \quad X = G(K, Y)$$

Le système de chiffrement est dit *symétrique* lorsque l'algorithme de déchiffrement se déduit très simplement de l'algorithme de chiffrement et inversement. Comme dans la plupart des cas[1] l'algorithme de chiffrement est connu de tous, voire normalisé, la sécurité de tels systèmes repose donc entièrement sur le secret de la clé *K* d'où leur qualification de *systèmes à clés secrètes*. Dans le monde numérique où nous nous plaçons, l'unité de chiffrement, *X*, constitue un *bloc* comprenant *n* éléments binaires, par exemple *n* = 64 ; on parle alors de chiffrement par blocs. Quand *n* = 1, on parle de chiffrement « bit à bit ». A titre d'exemple, examinons le cas d'un chiffrement réalisé élément binaire par élément binaire grâce à l'addition modulo-2 (symbole ⊕) et définie par : 0 ⊕ 0 = 1 ⊕ 1 = 0 et 0 ⊕ 1 = 1 ⊕ 0 = 1



[1] Exception faite des systèmes de chiffrement militaires

Ici, l'algorithme de déchiffrement est directement égal à celui du chiffrement puisque :

$$y = x \oplus k \quad et \quad y \oplus k = (x \oplus k) \oplus k = x \oplus (k \oplus k) = x \oplus 0 = x$$

Dans le cadre de la théorie de l'information[2], on peut démontrer qu'un tel système de chiffrement ne résistera à toute tentative de *cryptanalyse* (sera inconditionnellement sûr) qu'à la condition que la suite de clé soit purement aléatoire[3] et de même longueur que le texte clair. En d'autres termes, si cette condition est remplie, la connaissance du texte chiffré ne peut rien nous apprendre sur le texte clair. Mais la *gestion des clés* devient alors un fardeau insupportable : pour chaque transaction il faudrait acheminer vers le ou les destinataires une clé aléatoire différente et par des voies absolument sûres. Une telle lourdeur est admissible pour du chiffrement d'ambassade mais certainement pas pour le chiffrement en temps réel des énormes volumes de données de notre époque. Il faut alors se contenter de ce qu'il est convenu d'appeler une « sécurité calculatoire ». Dans notre exemple, les suites de clé sont produites par des générateurs de pseudo-aléa synchronisés et paramétrés par une même clé *K* de seulement quelques dizaines ou centaines de bits qui peut rester inchangée ou être changée à une fréquence déterminée en fonction des menaces ou des contraintes opérationnelles. Si le système est bien conçu[4] l'adversaire est confronté à une difficulté calculatoire équivalente à l'essai systématique de toutes les clés c'est-à-dire à environ 2^L essais si la clé utilisée a une longueur de L bits. Il suffit donc de se fixer une durée de résistance du chiffre et se baser sur les puissances de calcul les plus importantes du moment pour fixer L. Par exemple, une clé de 128 bits nécessiterait en moyenne plus de 10^{38} essais ce qui prendrait plusieurs milliers de milliards de millénaires avec des machines tournant à la cadence de l'ordre du petaflops (peta=10^{15}). Néanmoins, insistons sur le fait que rien ne peut prouver jamais, autrement que par l'expérience, qu'il n'existe pas une méthode de décryptement qui pourrait être plus rapide que l'essai de toutes les clés.

En matière de chiffrement par bloc, il existe des standards dont l'un des plus utilisés est l'AES ou Advanced Encryption Standard. Il remplace le très connu DES[5] jugé maintenant beaucoup trop faible. Il travaille sur des blocs de 128 bits avec des clés de 128 ou 256 bits. On peut également citer IDEA (International Data Encryption Algorithm) qui manipule des blocs de 64 bits avec des clés de 128 bits.

Systèmes asymétriques

Nous poursuivons maintenant avec les systèmes de chiffrement *asymétriques* encore appelés à *clé publique*. Un tel système est défini par une paire d'algorithmes *P* comme algorithme public et *S* comme algorithme secret et tels que *S* soit l'inverse de *P* sans pour autant qu'il ne soit possible de reconstruire facilement l'algorithme secret *S* à partir de la connaissance de l'algorithme public *P*. Ainsi, dans un réseau, le propriétaire du couple (*S*,*P*) pourra largement diffuser, par des canaux non sécurisés, la fonction publique *P* à tous ses correspondants qui pourront ensuite lui envoyer des messages *P*(X) chiffrés par l'algorithme public *P*, mais qu'il *sera le seul* à pouvoir déchiffrer grâce à sa fonction secrète *S,* puisque par construction *S*[*P*(X)] = X. On voit que l'on élimine ainsi toute diffusion préalable de clés secrètes ce qui facilite et améliore considérablement la sécurité du système d'information. Un tel dispositif est principalement utilisé pour transmettre les clés secrètes *K* des systèmes symétriques beaucoup plus aptes à traiter rapidement de forts volumes de données.

---

[2] Claude Shannon, 1948, *A Mathematical Theory of Communication*

[3] Système dit à masque jetable.

[4] Sans « backdoor » mais en sachant qu'il n'existe pas de méthode générale permettant de démontrer que ce type de système symétrique est « bien conçu » ce qui revient à s'en remettre à l'expérience et à la compétence des cryptologues.

[5] Data Encryption Standard, ne possédant que 56 bits de clé donc fragile vis-à-vis d'une attaque exhaustive des clés

Mais ce système asymétrique possède encore un autre avantage car en inversant les rôles il permet une véritable signature ou authentification numérique. En effet, ce même propriétaire du couple (S,P) peut aussi appliquer son algorithme secret S au texte X et diffuser $S(X)$ à tous les destinataires. Ces derniers pourront retrouver le texte initial X en utilisant la fonction publique car $P[S(X)]=X$; le fait d'obtenir le texte clair permet alors d'affirmer que seul le propriétaire de S a pu le créer ou l'envoyer ce qui authentifie donc bien l'origine du texte X. Il est aussi possible de combiner les deux opérations – chiffrement et authentification – si deux correspondants, A et B, échangent leurs propres clés publiques respectivement P_A et P_B ; par exemple A peut envoyer à B un message X doublement traité successivement par S_A puis P_B : $P_B[S_A(X)]$; le destinataire B déchiffrera l'ensemble en appliquant son algorithme secret S_B puis en appliquant l'algorithme public P_A de l'expéditeur A il obtiendra le message original X dont il pourra être certain qu'il provient bien de A.

Le système RSA

Mais comment peut-on faire en sorte que la connaissance d'un algorithme P ne puisse pas permettre de reconstituer (facilement) l'algorithme inverse S. Pour rendre calculatoirement impossible de retrouver S à partir de P on se base sur des problèmes notoirement complètement dissymétriques. Le plus connu d'entre eux est la factorisation de grands nombres en nombres premiers : il est facile de multiplier deux nombres premiers entre eux mais il peut être extrêmement difficile (au sens calculatoire) de factoriser en nombres premiers surtout si le nombre à factoriser est très grand. De ce constat fut issu dans les années 70 le ***système RSA***[6] (voir encadré). Le déchiffrement n'est possible que si l'on connait l'exposant de déchiffrement d tenu secret par le destinataire. Pour retrouver d à partir de l'exposant public de chiffrement e il faut résoudre

$$ed \equiv 1 \; mod (p-1)(q-1)$$

donc connaître p et q, donc être en mesure de factoriser le module de chiffrement public

$$n = p.q$$

Aujourd'hui, avec les algorithmes connus, le temps de calcul nécessaire à la factorisation augmente exponentiellement avec le nombre de bits de n. Pratiquement, RSA est utilisé avec des nombres de 1024 ou 2048 bits pour un haut niveau de sécurité. Mais rien ne prouve que l'on ne trouvera pas un jour des algorithmes plus rapides remettant alors en cause la sécurité des systèmes RSA. En particulier, avec l'algorithme de Shor[7] tournant sur un ordinateur quantique, il serait théoriquement possible de factoriser les nombres en un temps ne croissant que de façon polynomiale avec la longueur des clés ; mais pour l'instant, un tel ordinateur quantique n'existe pas et seules quelques expériences limitées à quelques bits ont été menées, notamment par IBM et Google.

RSA

Tout commence par la génération de deux grands nombres premiers p et q. Puis on calcule le *module de chiffrement* $n = p.q$ ainsi que l'indicatrice d'Euler en n (qui est le nombre d'entiers premiers avec n et inférieurs à n) qui vaut ici :

$$\varphi(n) = (p-1)(q-1)$$

On choisit ensuite un entier e qui soit premier avec l'indicatrice φ et inférieur à φ, appelé *exposant de chiffrement*.

On calcule l'entier d ou *exposant de déchiffrement*, inverse de e modulo φ c'est-à-dire tel que:

$$e.d \equiv 1 \bmod \varphi$$

Le couple (n,e) constitue la clé publique alors que d constitue la clé privée donc secrète.

Le chiffrement s'obtient par :

$$Y = X^e mod \; n$$

et le déchiffrement se fait par :

$$X = Y^d \; mod \; n$$

En effet :

$$Y^d = X^{ed} mod \; n$$

avec par construction :

$$ed \equiv 1 \; mod \; \varphi(n)$$

$$ed = 1 + \lambda\varphi(n)$$

où λ est un entier quelconque et finalement :

$$X^{ed} \equiv X^{1+\lambda\varphi(n)} = X \; mod \; n$$

d'après le théorème d'Euler.

Les courbes elliptiques

Ces courbes elliptiques sur corps finis permettent de réaliser des systèmes de chiffrement et aussi de signature à clés publiques. En simplifiant beaucoup, dans le domaine de la cryptographie,

[6] Acronyme dérivé du nom de ses inventeurs Rivest, Shamir et Adleman : « *A method for obtaining digital signatures and public-key cryptosystems* », *Communications of the ACM*, vol. 21, n° 2,1978, p. 120–126

[7] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Comput)er*

Une courbe elliptique, *E*, peut être vue comme une succession de points sur une courbe en deux dimensions du type :

$$y^2 = x^3 + ax + b \mod p$$

où *p* est un nombre premier (ou une puissance entière d'un nombre premier). Chaque point peut être atteint à partir d'un point donné appelé *générateur*. Une clé publique est un point *P*(x,y) de la courbe tandis que la clé privée correspondante est le nombre, *d*, en relation directe avec le nombre d'étapes à réaliser pour atteindre ce point à partir du point générateur *G* et symboliquement : $P = d.G$

La figure ci-contre est un exemple (très simple) de la construction géométrique de la clé publique pour $d = 3$

La clé publique est formée par l'ensemble des deux points (*G,P*) tandis que la clé secrète est *d*. En effet, connaissant *d*, construire *P* à partir du générateur *G* est facile à réaliser algébriquement tandis que retrouver *d* à partir du couple (*G,P*) revient à résoudre l'équation $P = d.G$ c'est-à-dire trouver le *logarithme discret* de *P* dans la base *G* ce qui est un problème considéré comme difficile qui requiert un temps croissant exponentiellement avec le nombre de bits de *d*. L'image géométrique le montre bien : pour trouver *d* il faut remonter vers *P* à partir de *G* en essayant un par un et successivement tous les points et combinaisons de points du groupe.

Il existe plusieurs cryptosystèmes basés sur les courbes elliptiques dont notamment les protocoles de chiffrement et de signature ElGamal[8] . Le système de signature fait l'objet d'un standard ECDSA[9]. Il existe également un protocole d'échange de clés[10] pour systèmes symétriques : les correspondants échangent leurs clés publiques et construisent chacun de leur côté la même clé secrète qu'ils utilisent ensuite avec un système symétrique classique.

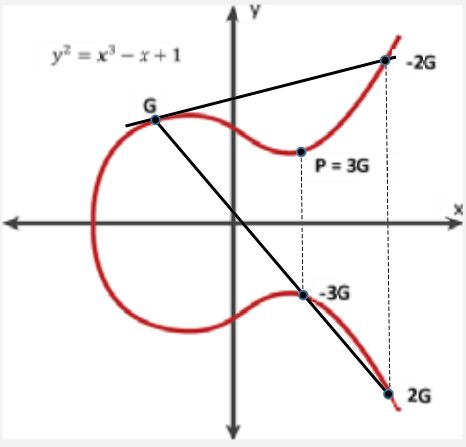
La figure ci-après est un exemple (très simple) de la construction géométrique de la clé publique pour $d = 3$ c'est-à-dire:

$P = G+G+G = (G+G)+G$

La première étape consiste à composer le générateur avec lui-même ce qui s'obtient par l'intersection avec la tangente en *G* dont on prend le symétrique, $2G$, par rapport à l'axe des *x*. La seconde étape est la composition du point $2G$ avec *G* pour avoir:

$P = 2G + G = 3G$

obtenu comme symétrique par rapport à l'axe des *x* de l'intersection de la droite joignant les points $2G$ et *G* avec la courbe elliptique. Dans la pratique, tous cela se fait algébriquement sur des entiers modulo *p* appartenant au corps F_p. Au sens de l'opération « addition » ainsi définie, l'ensemble des points forme un groupe abélien, $E(F_p)$, de cardinal (ou ordre) *q* relié à *p* par le théorème de Hasse et toujours calculable par l'algorithme de Schoof ; en outre, ce groupe est cyclique ce qui implique qu'en partant d'un générateur quelconque et en poursuivant les compositions successives, tous les points du groupe sont parcourus.



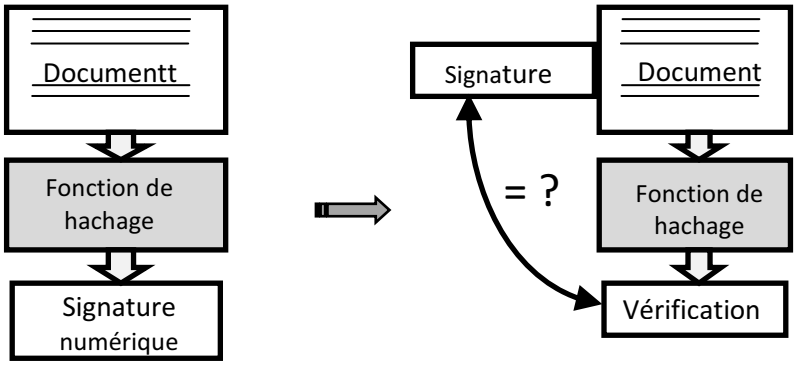
[8] T.ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE,1985

[9] X9.62-1998, *Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*

[10] Protocole Diffie-Hellmann. Malheureusement il ne résiste pas à l'attaque dit du « man in the middle »

Fonction de hachage

Il est important de pouvoir vérifier à tout moment qu'un document numérisé n'a pas subi d'altération volontaire ou accidentelle. La façon la plus courante d'y parvenir est de créer une « empreinte » ou « signature » numérique d'une longueur fixe indépendante de celle du texte à signer et telle que la moindre modification du texte entraîne automatiquement une modification de la signature. Une telle image du document s'obtient grâce à une fonction, *H*, dite de « hachage ». Elle découpe le document numérisé en une série de plus petites séquences par exemple des mots de128 bits chacun. Puis chaque mot est chiffré par un algorithme symétrique dont la clé est fournie par le mot chiffré précédent ; le premier mot a pour clé une clé de 128 bits qui peut être connue ou secrète. Donc quelle que soit la longueur du document on obtient, au bout du compte, un mot de 128 bits constituant la signature. La vérification de la signature donc de l'intégrité du texte, s'obtient en appliquant de nouveau la même fonction de hachage et en comparant le résultat obtenu à la signature numérique accompagnant le document. On exige évidemment de la fonction de hachage qu'elle soit telle qu'il soit impossible (ou infiniment peu probable) de trouver un autre texte présentant la même signature ; on dit qu'elle doit être résistante aux collisions. Si ce n'était pas le cas alors il serait possible de créer des faux. Globalement, en désignant par *M* le document à signer, par *K* le premier mot clé et par *C* la signature :



$$C = H(K, M)$$

Si le paramètre *K* est connu i.e. fait partie constante de la fonction de hachage, la signature ne permet de vérifier que l'intégrité de l'information. Si au contraire *K* est une clé secrète connue seulement de l'émetteur et du récepteur, alors l'empreinte *C* permet aussi une authentification de l'émetteur : si la signature est vérifiée avec succès, c'est bien le détenteur de la clé secrète *K* qui a pu l'écrire. Mais une telle authentification est nettement moins forte que celle obtenue avec une procédure à clef publique car rien n'empêche le destinataire de forger et signer tout message qu'il souhaite puisqu'il détient également la clé qui permet aussi bien de signer que de vérifier.

Les fonctions de hachages sont souvent normalisées donc parfaitement connues. Le standard le plus répandu est le SHA-1 qui fournit un condensé (signature) de 160 bits sur des textes de longueur maximal de 2^{64} bits. Il tend à être remplacé par le standard SHA-2 considéré comme beaucoup plus sûr ; par exemple, la version SHA-256 fournit des signatures de 256 bits pour des textes de longueur allant jusqu'à 2^{64} mais le nombre d'opérations nécessaire pour obtenir une collision atteint le chiffre astronomique de 2^{128}.

En route pour la seconde partie

Nous voici suffisamment armés pour aborder la seconde partie de « la cryptologie au quotidien » et que le lecteur se rassure elle sera nettement moins technique que la première : nous y traiterons des services et applications pratiques de la cryptologie. Nous aborderons le sujet important des « certificats » et tiers de confiance. Nous examinerons les différences entre le chiffrement de voies (les couches transport ou réseau) et le chiffrement de bout en bout (au niveau des couches application) et leurs implications dans les compromis à faire entre la vie privée et la sécurité publique. Nous traiterons aussi de la sécurisation des moyens de paiement classiques comme la carte VISA ou moins classiques comme ceux offerts par les cryptomonnaies. Nous verrons également que la gestion des clés reste toujours un point faible dans le cadre de la sécurité des systèmes d'information et comment la physique quantique peut apporter de nouvelles solutions. Enfin, pour conclure nous dirons quelques mots de la bataille féroce qui s'annonce entre les systèmes à clés publiques et les futurs ordinateurs quantiques capables, en théorie, de s'attaquer à la factorisation des grands nombres ou à la résolution des logarithmes discrets beaucoup plus efficacement que les algorithmes actuels tournant sur nos ordinateurs classiques.

Dans le prochain numéro, vous trouverez la seconde partie de cet article.

La titrisation au secours du crédit

(suite de la page1)

Le but de la titrisation.

La titrisation permet aux banques ou à des organismes financiers de se refinancer en cédant un portefeuille de créances à une société ad hoc (société de titrisation ST, encore appelée SPV Special Purpose Vehicle) ou à un fonds commun de titrisation (FCT).
Cela leur permet :
-de mobiliser immédiatement la trésorerie d'un actif
-de trouver des fonds à un coût inférieur à ce qu'elle pourrait trouver elle-même sur le marché.
-de céder le risque
-d'améliorer leurs ratios prudentiels.

Mobiliser immédiatement la trésorerie d'un actif

Dans la mesure où un détenteur de créances cède un portefeuille de créances à une société ad hoc ou à un FCT, le cédant reçoit la contrepartie des flux financiers générés par les créances, immédiatement, alors que ceux-ci ne se matérialiseront que dans le futur et au fur et à mesure des remboursements des mensualités par le débiteur.

Trouver des fonds à un coût inférieur à ce qu'elle pourrait trouver elle-même sur le marché.

Du fait de leur cession, les créances quittent l'actif de la banque ou de l'établissement financier pour se retrouver à l'actif de la ST ou du FCT. De ce fait le risque lié aux créances est parfaitement individualisable et homogène. Il est possible de l'évaluer indépendamment du risque d'autres actifs. Par exemple le risque sur les emprunts hypothécaires est évalué à 0.5% des prêts.
De ce fait par la technique du "tranching" (voir plus bas) et par la mise en place de garanties (garanties bancaires, assurances, surdimensionnement, conservation de 5% des obligations émises par la ST ou le FCT, etc.), il est possible de faire porter le risque du financement de ces actifs par certains investisseurs qui seront conscients du risque qu'ils prennent et seront rémunérés pour cela. Si les débiteurs font défaut ce sont ces investisseurs qui perdront leur mise en premier de façon définitive. C'est pour cette raison que l'on parle de titrisation sans recours. Ce mécanisme va permettre d'émettre des obligations de risque différent qui seront notées de façon différente. Ainsi on essayera d'émettre 70 à 90 % d'obligations notées AAA (obligations senior), des obligations mezzanines notées par exemple AA, des obligations junior notée BB et ainsi de suite. Il peut y avoir de très nombreuses tranches. Ce mécanisme est appelé le « tranching ». Quel en est l'avantage ? Supposons que la dette d'une banque cédante soit notée A+ et qu'elle peut emprunter disons à 2, 7%. Grâce au dispositif de la titrisation, elle va pouvoir bénéficier de la notation AAA sur une grande partie de l'emprunt et payer nettement moins cher, disons 1,90%. Bien sûr les frais de la structure seront à ajouter, mais sur des montants importants l'opération en vaut la peine.

Céder le risque

La cession de créance et le mécanisme tel qu'il a été décrit, implique que le risque est cédé aux investisseurs et n'est plus (tout au moins fortement) à la charge du cédant. Ceci entraîne de facto l'amélioration des ratios prudentiels.

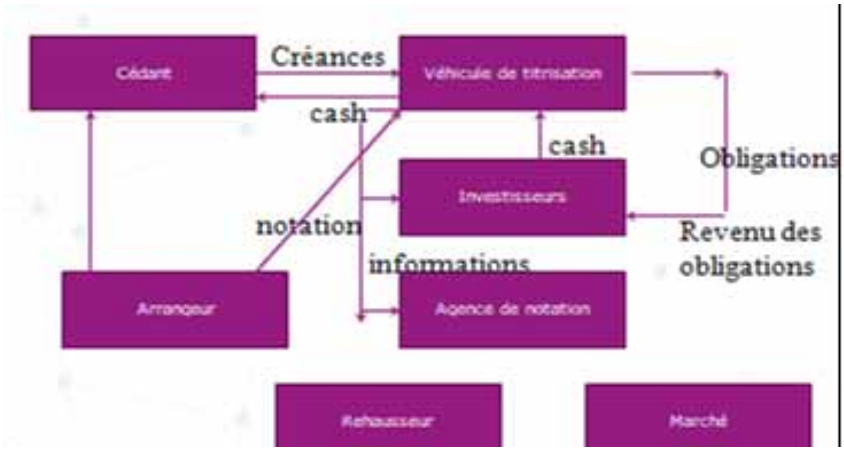
Améliorer les ratios prudentiels

Du fait de la cession de créance, le montant du risque pondéré est diminué et le besoin de capitaux propres exigés par l'application du ratio Mc Donough[11] et des ratios complémentaires comme les coussins, le Tlac[12] et ainsi de suite se réduit. Il en est de même du ratio de levier ainsi que des ratios de liquidité qui sont améliorés.

Conclusion

La titrisation (financement sans recours) est pour les banques et les organismes financiers un moyen efficace de trouver des capitaux et de réduire leur risque, ce qui dans la période actuelle d'obligation de renforcement des capitaux propre des banques est un atout considérable.
D'autres techniques de titrisation existent comme la titrisation synthétique où la banque ou l'organisme financier ne cèdent pas les créances mais uniquement le risque. En particulier une plateforme expérimentale a été créée récemment entre BNPPARIBAS et la Banque Européenne d'Investissement (BEI) pour le financement des PME et des ETI.
Toujours avec BNPPARIBAS une plateforme de titrisation du commerce international a été mise en place.[13]

Schéma d'une titrisation



En 2018, 2 formations approfondies portant sur la titrisation seront effectuées par l'auteur : 11 au 12 juin 2018 et 3 au 4 décembre 2018. Renseignements : http://www.afges.com/formations-catalogue/technique-de-titrisation/

[11] Banque des Règlements Internationaux (BRI) https://www.bis.org/bcbs/publ/d424_inbrief.pdf

[12] Voir article de l'auteur http://www.afges.com/le-tlac-total-loss-absorbing-capacity-en-bref/

[13] Voir article de l'auteur http://www.afges.com/titrisation-le-financement-du-commerce-international/

Stratégies & Information

« Seul le vide pénètre là où il n'y a pas de faille » Lao-Tseu

Stratégies et Informations

Lettre d'analyse économique et de cognitique financière Relative à l'évolution des marchés

Éditée par SIGRE PRESSE
1, Rue Rennequin
75017-Paris
Tel :0033147665058
Fax :OO33142277199

Directeur de la Publication :
Andrea Brignone

Rédaction :
Andrea Brignone
Laure Brignone
Anne de Canecaude
(Los Angeles)
Herbert Groscot
Edouard Hostin
Joël Lebidois
Yuri Rudakovsky
(Moscou)
Et
Janus

Lettre publiée sous forme électronique

ISSN-1254-8103
Prix au numéro : 20 €
Abonnement :12 numéros 200€

TABLEAU DE BORD DU COMMERCE INTERNATIONAL

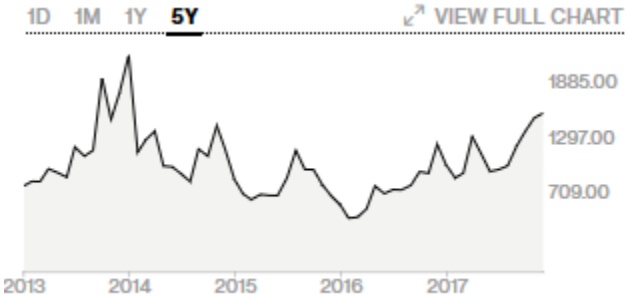
L'indice Harpex (Taux de fret des conteneurs)

Origine :Harper Petersen & Co

L'indice Harpex se maintient à un niveau (481) loin de son plus bas indiquant que l'échange de produits manufacturés se maintient malgré les menaces protectionnistes.

Le Baltic Dry Index

Origine : Bloomberg



Le Baltic Dry Index se trouve au plus haut (1547) depuis 2014 indiquant de forts échanges dans le domaine des matières premières. C'est un index avancé de l'évolution future de la conjoncture car il indique que les producteurs commandent en prévision de productions futures.

La hausse concomitante des deux indices indique que l'économie mondiale est en croissance et qu'à court terme (3 à 6 mois) cette croissance a de fortes chances de continuer.