LES NANOTECHNOLOGIES DANS L'INDUSTRIE ÉLECTRONIQUE

L'INNOVATION APPLIQUÉE À LA SÉCURITÉ

Serge Maginot (82)

Initialement développeur d'une technologie innovante de conception de composants électroniques asynchrones, la société Tiempo s'est focalisée depuis 2010 sur la fabrication de circuits intégrés pour applications fortement sécurisées telles que les cartes à puce bancaires avec et sans contact, les documents d'identification et les éléments sécurisés pour applications mobiles ou M2M. Rencontre avec l'un des fondateurs et Président de Tiempo, Serge Maginot (82).

Pourquoi se concentrer sur les produits sécurisés ?

Au départ, notre objectif était d'industrialiser une technologie innovante de conception de circuits intégrés. Nous avons mis au point un flot de conception de circuits dits « asynchrones », c'est-à-dire fonctionnant sans aucune horloge et dont chaque opération est contrôlée localement par un protocole basé sur des rendez-vous (« handshakes »). Cette méthode de conception originale permet de réaliser des circuits qui adaptent automatiquement leur vitesse à l'énergie disponible et qui sont ainsi très robustes, réactifs et efficaces en environnement à forte variabilité énergétique. Nous avons ensuite utilisé ce flot (unique sur le marché de microélectronique) pour concevoir et commercialiser une famille de circuits intégrés pour applications sécurisées et/ou sans contact. Nous nous concentrons d'ailleurs aujourd'hui sur l'industrialisation de notre premier produit, TESIC-SC, un circuit microcontrôleur sécurisé à interface duale (avec et sans contact) pour cartes à puce bancaires et documents d'identification.

Nous avons décidé de nous spécialiser sur ces produits sécurisés car notre technologie et notre flot de conception permettent de réaliser des circuits particulièrement efficaces pour ce type d'applications. En effet, sachant que l'énergie envoyée au circuit de la carte bancaire sans contact par le lecteur de cartes augmente lorsque la distance entre carte et lecteur diminue, les circuits conçus dans notre technologie asynchrone vont instantanément augmenter leur vitesse de traitement lorsqu'ils se rapprochent du lecteur, ce qui leur permet d'exécuter des transactions sécurisées dans un temps globalement beaucoup plus court que les circuits traditionnels, avec horloge. De plus, le profil de consommation énergétique de ces circuits, beaucoup plus « aplati » que celui des circuits synchrones qui présentent des pics de consommation dus aux horloges, les rends beaucoup plus résistants aux attaques de sécurité. Les circuits de Tiempo permettent donc d'exécuter des transactions de manière plus sécurisée, plus robuste et à une vitesse plus élevée dans les conditions énergétiques variables que sont celles des applications sécurisées sans contact.

Comment garantir un très haut niveau de sécurité pour des marchés aussi sensibles que les cartes bancaires ou les passeports ?

Si tout le monde est familier avec le concept de cyber-attaques ou de piratage informatique, au niveau logiciel, via Internet par exemple, moins connus mais tout aussi réelles sont les attaques sur les matériels électroniques, au niveau du hardware.

Les puces des cartes bancaires échangent ainsi avec le lecteur de cartes des données qui sont chiffrées puis déchiffrées au moyen de clefs de chiffrement/déchiffrement, certaines de ces clefs étant stockées dans le circuit lui-même. Ceci est également valable pour les informations stockées et traitées dans les circuits des documents d'identification, comme les puces des passeports biométriques.

Or, il existe des techniques de piratage hardware – on parle d'attaques hardware - qui permettent d'extraire de telles informations des circuits intégrés. L'analyse différentielle de dizaines ou de centaines de milliers de courbes de consommation électrique d'un circuit en fonctionnement (exécutant des chiffrements) permet d'extraire des constantes de ce circuit (comme les clefs de chiffrement). D'autres techniques d'attaques mettent en œuvre des insertions de fautes dans les circuits, au moyen de lasers ou de glitchs de tension, l'observation des résultats fautés pouvant révéler des informations sur les constantes du circuit.

Pour empêcher ces attaques en les rendant trop complexes et donc trop coûteuses en matériel et en effort de piratage, on intègre des contre-mesures de sécurité dans les circuits intégrés pour que ces derniers détectent automatiquement les attaques (détecteurs de lumière, de température, de glitchs...) et interrompent aussitôt leur fonctionnement, et pour que leur fonctionnement soit « brouillé », c'est-à-dire plus difficilement observable lors d'attaques par analyse de consommation électrique. Nous avons développé et breveté à Tiempo plusieurs types de contremesures particulièrement efficaces grâce à une implémentation en logique asynchrone, dont une technique d'insertion de délais aléa-

toires pour « aplatir » et « brouiller » les courbes de consommation électrique, technique particulièrement efficace car nos circuits, sans horloge, sont insensibles aux délais.
Enfin, tous les circuits conçus par Tiempo sont certifiés ISO15408 Critères Communs EAL5+ et EMVCo.

Quels sont les autres marchés visés ?

Dès 2009/2010, nous avons compris combien notre technologie serait déterminante pour le marché des produits sécurisés, et notamment pour le marché des cartes bancaires à interface duale (avec et sans contact). Mais le marché de la sécurité, en forte croissance, est beaucoup plus vaste. Outre les produits pour cartes bancaires et documents d'identification, le besoin de sécuriser les transactions et les communications de données devient critique dans plus en plus d'applications : paiement par téléphone et smartphone, protection des droits sur les contenus numériques (comme les cartes à puce pour décodeurs satellite ou programmes cryptés, où les enjeux économiques sont considérables), communications « machine-to-machine » (M2M) dans l'Internet des Objets, protection de la confidentialité des données médicales échangées entre appareils portatifs/sans fil et bases de données, etc. Tiempo vise tous ces domaines où l'on assiste à un besoin accru en chiffrement complexe de données transmises et en matériel électronique sécurisé réalisant ces chiffrements/déchiffrements et résistant aux attaques hardware.

Travaillez-vous aussi à une déclinaison de votre technologie appliquée au secteur de la santé ?

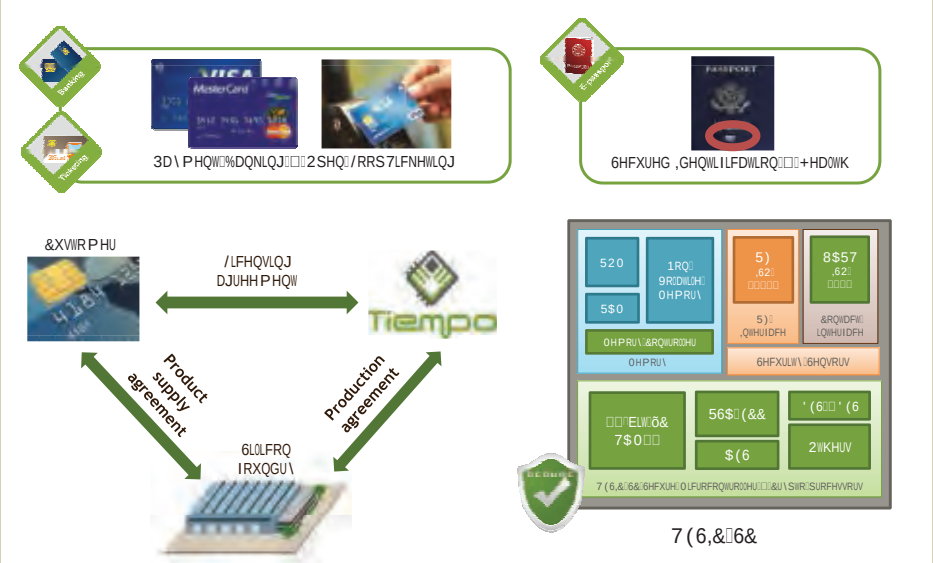
Les prochaines applications visées après le bancaire et l'identification sécurisée seront certainement dans le domaine médical. C'est fondamental car les données médicales doivent être absolument protégées et il y existe de plus en plus d'appareils portables connectés pour des applications de bien-être ou de santé. Sur ce type d'applications, outre les besoins en sécurité, le problème de la gestion de la batterie est également essentiel, notamment pour la surveillance médicale des personnes âgées. Avoir une technologie qui permet d'ajuster les performances en fonction de l'énergie disponible nous donne, en plus de la sécurisation, un avantage concurrentiel certain sur l'aspect énergétique.

Quel est votre business model ?

Notre premier business model suivait un modèle horizontal, adressant tout type d'applications de circuits intégrés asynchrones, et consistait en vente de licences de logiciels de CAO et de blocs de propriété intellectuelle aux sociétés de microélectronique concevant et fabricant des circuits intégrés. En 2010, nous avons changé notre business model pour un modèle vertical, se spécialisant sur une famille d'applications spécifiques, les applications sécurisées. Notre société industrialise et commercialise maintenant des circuits intégrés, nos clients étant les sociétés fabricant des systèmes avec ces circuits.
Tiempo ne possède pas de salle blanche de production mais fait fabriquer ses circuits dans le cadre d'un partenariat avec une fonderie italienne. Notre produit TESIC-SC est sous contrat de licence avec cette société qui peut fournir directement en silicium le client final, lui même sous contrat de licence avec Tiempo qui touche des royalties sur l'ensemble des circuits vendus.
Dans la mesure où nous restons une petite société, associée à des salles blanches, elles-mêmes de taille moyenne et dotées de coûts opérationnels plus réduits, nous arrivons à proposer une offre commerciale très compétitive par rapport aux grandes sociétés de microélectronique.

Quels sont vos objectifs et vos perspectives de croissance ?

Le marché des circuits pour cartes bancaires et documents d'identification est un marché difficile, très spécialisé et avec de fortes exigences, notamment sur la sécurité. Les normes (Critères Communs, EMVCo) y sont aussi complexes que strictes et les leaders sont généralement de grandes sociétés de microélectronique (NXP, Infineon, ST, Samsung..). Il y a également quelques sociétés de taille plus modeste, comme Tiempo, mais il existe aujourd'hui dans le monde moins de dix sociétés capables de concevoir et de produire des circuits répondant aux normes de sécurité aussi exigeantes que les Critères Communs EAL5+ ou EMVCo.
Chez Tiempo, nous avons travaillé plus de trois ans pour rendre notre société et nos produits compatibles avec ces normes, ce qui nous donne un avantage certain par rapport à nombre de sociétés de microélectronique, notamment chinoises, qui voudraient entrer sur le marché de la sécurité. Nous savons également que cet avantage est temporaire, ce qui nous impose d'être toujours plus innovant et exigeant sur le plan technique comme sur notre politique commerciale et de gestion de nos coûts de production. Ce qui nous intéresse aujourd'hui, c'est l'idée qu'il y ait, à côté des géants de la microélectronique, une place pour une petite entreprise capable d'avoir une offre flexible et compétitive en circuits intégrés sécurisés et certifiés Critères Communs. Au-delà de la société Tiempo, nous avons aussi envie de défendre l'idée qu'il est important de conserver et de développer une industrie de la microélectronique européenne, tout particulièrement sur le marché de la sécurité. ■



www.tiempo-secure.com