Recherche sur crédits incitatifs - Appel 2004

FICHE DESCRIPTIVE

TITRE DE L'ACTION Carte à puce ouverte
NOM DE CODE OpenSmartCard

RESPONSABLE DE L'ACTION Yves MATHIEU
COMPOSITION DE L'EQUIPE ET ORIGINE
- **ENST (70 %)** : Sylvain GUILLEY, Philippe HOOGVORST, Jean LEROUX-LES-JARDINS, Philippe MATHERAT, Yves MATHIEU, Renaud PACALET, Jean PROVOST
- **ENST Bretagne (30 %)** : Ronan KERYELL

MOTS CLES
- **Disciplines** : 1.x.x et 3.x.x
- **Application / Activité** : x.1.x et x.2.x
- **Sous-application / Activité** : x.1.1 et x.2.3

RESUME

Les vulnérabilités des circuits électroniques contre les attaques matérielles compromettent la sécurité des infrastructures qui s'appuient sur des cartes à puces et freinent par conséquent le développement du marché de l'électronique servant de support aux réseaux d'intelligence ambiante de demain.

Ce projet a pour ambition de fournir des solutions au problème de la sécurité du matériel. Des contre-mesures concrètes contre les attaques sur les canaux cachés (SPA, DPA et EMA) et contre les attaques sur les accès aux mémoires seront proposées et implémentées dans un circuit expérimental, puis dans une carte à puce.

Les résultats, validés par des expériences menées sur la carte à puce, seront publiés avec l'intégralité du code ayant servi à concevoir la carte à puce. Cette approche permettra d'imposer un nouveau modèle pour la sécurité (ouverture du matériel), d'établir un standard *de facto* pour la conception du matériel de sécurité et d'infléchir les spécifications des futurs processeurs et cartes à puce.

BUDGET TOTAL DE L'ACTION 90 000 €
BUDGET DEMANDE AU GET 40 000 €
AUTERS SOURCES DE FINANCEMENT **Contrat PACA / STMicroelectronics** : conception (2+1 CDD sur 6 mois) et fabrication d'un circuit (Total : 50 000 €). **Collaboration avec Inseal**, start-up incubée à l'ENST, qui développe d'un système d'exploitation libre pour cartes à puce (`http://www.inseal.com`).

	ENST + ENSTB
Fonctionnement	Fabrication d'un ASIC via le CMP (4 500 €), déplacements (4 000 €).
Investissement	Support de la carte à puce (1 000 €), appareils de mesure et d'attaque sur la carte à puce (2 000 €), logiciels divers (900 €).
Personnel	Un ingénieur de développement HW/SW (10 hommes × mois : 19 800 €), un stagiaire pour réaliser les mesures (5 hommes × mois : 7 800 €).
Total	40 000 €

DESCRIPTIF DE L'ACTION

1. Contexte scientifique

Le projet de carte à puce ouverte a comme ambition de développer et de rendre publique une méthodologie de conception de *systèmes sur puces* (Systems on Chip, ou SoC) sécurisés. Des contre-mesures contre les vulnérabilités connues des dispositifs de calcul matériels seront proposées. Des solutions de mise en œuvre de ces contre-mesures seront intégralement publiées. Un circuit expérimental (financé par contrat PACA et STMicroelectronics) ainsi qu'une carte à puce utilisant ces solutions seront fabriqués.

De plus en plus de circuits électroniques sont utilisés de manière éparse dans notre environnement afin de créer des réseaux d'*intelligence ambiante*. Ces circuits communiquant répondent aux besoins d'auto-gestion et d'auto-diagnostic des infrastructures, d'automatisation de certaines tâches, de fluidification des interfaces hommes-machines, *etc.*

Ces circuits s'organisent en réseaux ouverts dont il faut assurer la sécurité. Nous connaissons aujourd'hui les cartes à puces, et nous savons que c'est l'effort investi pour les protéger contre les attaques malveillantes qui a rendu possible leur essor. Une autre caractéristique des cartes à puce qui leur confère un haut niveau de sécurité est l'intégration de l'ensemble du système sur un même support ; cela complique les attaques intrusives.

Néanmoins, un système intégré comme une carte à puce présente *a priori* plusieurs failles majeures de sécurité : les attaques exploitant les canaux cachés, comme la SPA, la DPA ou l'EMA [5], permettent de dévoiler par une observation extérieure non intrusive le fonctionnement interne du circuit. Par ailleurs, les cartes à puces étant des systèmes complexes, de nombreuses vulnérabilités peuvent résulter des erreurs (*bugs*) de conception. Cependant, il n'existe que peu d'information sur la façon de concevoir un SoC, comme une carte à puce, qui prenne en compte aussi bien une étanchéité du matériel et une architecture pensée pour la sécurité.

Or la sécurité d'un système ne peut véritablement être garantie que si son architecture est rendue publique, de telle sorte les vulnérabilités résiduelles soient critiquées.

Ce projet est à notre connaissance une initiative unique : actuellement, la sécurité des circuits électroniques est essentiellement basée sur le secret des techniques de conception pour la sécurité, techniques souvent facilement contournables (modes de debug, obfuscation des données). Le projet contribuerait à instaurer une méthode publiquement certifiée et reconnue comme sûre dans la conception de circuits *critiques* en termes de sécurité.

Les recherches sur les processeurs sécurisés datent des années 1980 et celles sur les architectures résistantes aux attaques sur les canaux cachés de 1998. Aucune proposition d'architecture matérielle et d'API logicielle, complètes et garanties sûres, n'a été publiée à ce jour.

Des études sur des sujets connexes sont actuellement menées dans divers organismes, privés ou publics. Des processeurs sécurisées sont notamment produits et vendus (Dallas Semiconductor) et font l'objet de brevets (R.M. Best, US 04278837 et US 04465901). Les attaques sur le matériel intéressent de nombreux laboratoires, dont *TAMPER* à Cambridge [3] et le *Side Channel Laboratory* à Graz [2]. Les équipes

de recherche impliquées dans le projet `G3Card` (`http ://www.g3card.org/`) avancent des propositions pour l'architecture de la prochaine génération de cartes à puces sécurisées. Ils préconisent notamment l'utilisation de la logique asynchrone. La recherche sur la sécurité des systèmes matériels est une discipline en plein épanouissement, comme en témoigne en France le positionnement de la DCSSI comme acteur réglementaire ou au niveau international par le succès chaque année plus important de la conférence CHES (Cryptographic Hardware and Embedded Systems).

2. Contenu scientifique

Les compétences développées dans ce projet relèvent des domaines de l'électronique et de l'architecture des processeurs (ou des SoC en général).

Des solutions innovantes d'architecture micro-électronique et d'architecture de systèmes sécurisés seront proposées suivant une démarche en deux temps. Dans un premier temps, les vulnérabilités, avérées ou potentielles, seront étudiées. On décrira aussi précisément que possible leur cause et les conditions de réalisation pratique d'une attaque. Partant de ses données, on élaborera dans un deuxième temps un jeu de contre-mesures, qui sera implémenté dans un premier circuit expérimental (contrat PACA et STMicroelectronics). On développera également un protocole de vérification du niveau de sécurité d'un circuit. Ce protocole délivrera une qualification pour un certain niveau de confiance des critères communs [1].

Des expériences menées sur le circuit expérimental permettront d'itérer la démarche : en fonction des résultats mesurés sur le premier circuit, on validera ou invalidera les premières solutions embarquées. Prenant en considération les avantages et les défauts du premier circuit, un second circuit, pour carte à puce cette fois, sera conçu et fabriqué en fin de projet.

Plus spécifiquement, pour ce qui concerne la sécurité physique du matériel, on s'interrogera sur l'origine des fuites d'information rendant possibles les attaques sur canaux cachés. Les contre-mesures viseront à régler le problème à la source : l'objectif est d'inventer une électronique étanche. Par ailleurs, on cherchera à rendre inefficaces les attaques par injection de fautes, que cela soit pour perturber le fonctionnement normal du dispositif ou pour le détériorer. On proposera en outre des mécanismes de détection d'une manipulation suspecte.

On proposera également des architectures de processeurs incluant des mécanismes de protection contre les attaques classiques :

- chiffrement des données et des instructions,
- authentification des données provenant des mémoires,
- protection des zones mémoires allouées à des processus différents.

On pourra proposer d'autres contre-mesures répondant à des attaques (connues ou à inventer) plus spécifiques, comme le rejeu.

Le travail de sécurisation des fuites d'information électronique s'appuie sur des études réalisées à l'ENST. On a d'ores et déjà montré que le rapport signal sur bruit de l'attaque de DPA est d'autant plus élevé que les algorithmes de chiffrement sont robustes. De plus, on pressent que l'attaque est réalisable sur tout cône logique, quelque soit sa profondeur ou sa largeur ; la menace que constitue la DPA ne peut donc pas être éludée. Des travaux basés sur la simulation électrique ont mis en évidence les conditions de réalisation de la DPA. La conclusion de ces expériences est que l'unique manière de prévenir les attaques sur les canaux cachés est de supprimer lesdits canaux. Des structures en transistors de portes sécurisées, avec leur dessin

des masques, ont été développées. Il reste à les optimiser et à étudier leur intégration dans un flot de conception automatisé, basé sur des outils commerciaux usuels de CAO (Conception Assistée par Ordinateur).

Les architectures de processeurs sécurisés émanent des travaux de l'ENST Bretagne sur le processeur CryptoPage [4]. Ce processeur est conçu pour résister à toutes les attaques connues sur les accès mémoire. Son implémentation matérielle, à base d'un contrôleur ou d'un processeur libre, reste à étudier et à réaliser. Les logiciels permettant de le programmer sont également à développer.

3. Conformité de la proposition aux critères de sélection

Le projet de carte à puce ouverte associe les groupes SEN (Systèmes Intégrés Numériques) de l'ENST Paris, LIT (Laboratoire d'Informatique et de Télécommunications) de l'ENST Bretagne et SOC (System On Chip) de l'ENST Sophia. Ce projet est par ailleurs à la confluence de cinq thématiques de recherches au GET : la sécurité, les architectures de systèmes, l'électronique numérique intégrée, la logique asynchrone et les cartes à puces. Il permet de réaliser le lien entre les sujets de recherches d'équipes différentes, propose un objectif finalisé commun (la carte à puce) et suscite de nouvelles problématiques transverses.

Une ambition du projet est de mettre un place un nouveau modèle pour la sécurité des crypto-processeurs. L'ouverture engendrée par la libre distribution des sources (dessins de masques, code source de la description du matériel et des API logicielles) s'oppose à la fermeture des solutions propriétaires. Le bénéfice à retirer de cette approche est triple :

1. imposer un modèle,
2. établir un standard *de facto*,
3. infléchir les spécifications des futurs processeurs et cartes à puces.

La fabrication d'une carte à puce conforme aux propositions émanant du projet sera garante de leur validité. Par ailleurs, on veillera à utiliser autant que possible des outils libres ou, à défaut, des outils suffisamment répandus, afin de s'assurer que l'utilisation des données et des codes sources fournis sont exploitables par un très large public.

La démarche d'ouverture du projet est propice à des partenariats, aussi bien avec des entreprises qu'avec l'état. Le travail de conception et la fabrication du premier circuit expérimental est déjà financé par un contrat avec la région PACA et le fondeur STMicroelectronics.

Le projet s'inscrit dans une triple perspective :

1. informer et sensibiliser sur les attaques portant sur le matériel, pouvant mettre en défaut la sécurité d'entreprises ou d'organismes (par exemple suite au piratage d'un système de PKI basé sur des cartes à puces),
2. contribuer à mieux protéger les grandes infrastructures, par des propositions techniques concrètes et par la réalisation de deux prototypes de cartes à puce sécurisées,
3. promouvoir l'ouverture de l'électronique pour la sécurité.

Les deux premières perspectives sont des thèmes prioritaires de l'appel à propositions de recherche sur crédits incitatifs GET 2004.

4. Calendrier détaillé de l'action et nature des résultats fournis

Les délivrables sont indiqués **en gras** dans le calendrier de l'action ci-dessous.

Dates	Description
	CAO sécurisée
Janvier 2004	Fourniture d'une bibliothèque de cellules sécurisées (synchrones et asynchrones).
	Publication des dessins des masques.
Février 2004	**Publication d'une méthode de placement et de routage des cellules sécurisées**.
	Processeur sécurisé
Janvier 2004	Spécifications du processeur (ou du contrôleur) sécurisé.
Février 2004	**Architecture matérielle du processeur sécurisé**.
	Intégration dans le circuit expérimental (premier circuit)
Mars 2004	Spécifications générales du circuit expérimental (modules à inclure, type d'architecture du SoC).
Mars - Avril 2004	Conception du circuit intégré (ASIC).
Juin 2004	**Fabrication du circuit** (financement par le contrat PACA et STMicroelectronics).
	Exploitation du circuit expérimental (premier circuit)
Juillet 2004	Test du circuit.
	Manipulations sur le circuit expérimental : mesures de sécurité et réalisation d'attaques.
Août 2004	Conclusions (positives ou négatives) quant aux premières idées.
	Réalisation d'attaques actives et/ou destructives sur le circuit expérimental.
	Conception de la carte à puce (deuxième circuit)
Septembre 2004	Éventuelle modification de la bibliothèque de cellules sécurisées et redéfinition du flot de conception.
	Amélioration du processeur sécurisé et de son architecture, utilisation de l'OS jayacard (`http://www.jayacard.org/`) d'Inseal.
	Développement du protocole de qualification d'un circuit contre les critères communs [1].
Octobre 2004	Mise à jour des spécifications du circuit expérimental.
	Application des spécifications mises à jour à la carte à puce et conception du circuit de celle-ci.
Novembre 2004	**Fabrication du deuxième circuit** (financement par le crédit incitatif GET).
	Exploitation de la carte à puce (deuxième circuit)
Décembre 2004	Test, encartage et répétition des expériences.
	Conclusions quant à l'effectivité des modifications apportées par rapport au premier circuit.
Janvier 2005	Fin des mesures, **rédaction d'un compte-rendu** et **publication sur internet d'une archive des codes sources de la carte à puce**.

Nota bene : le projet pourra éventuellement dépasser la durée d'un an en fonction des fenêtres et du temps de fabrication des circuits.

5. Budget détaillé

Fonctionnement

Les frais de fonctionnement couvrent la fabrication du circuit de la carte à puce (4 500 €) ainsi que les déplacements Bretagne↔Paris et Sophia↔Paris (4 000 €).

Investissement

La conception et la fabrication du circuit expérimental sont déjà pris en charge par un contrat avec la région PACA et STMicroelectronics.

Les investissements restant concernent les dépenses suivantes :

- Support de la carte à puce : 1 000 €,
- appareils de mesure et d'attaque sur la carte à puce : 2 000 €,
- logiciels (CAO et divers) : 900 €.

Personnel

Le projet comportant la réalisation de deux plate-formes, à savoir un circuit expérimental et une carte à puce, un ingénieur de développement logiciel et matériel est indispensable à partir du mois de Mars 2004.

Par ailleurs, un stagiaire sera en charge des mesures (test et attaques sur les cartes) après réception du premier circuit (juillet-août-septembre 2004) et après réception du circuit de la carte à puce (décembre 2004-janvier 2005).

Résumé

	Budget
Fonctionnement	Fabrication d'un ASIC via le CMP (4 500 €), déplacements (4 000 €). **Total** : 8 500 €
Investissement	Support de la carte à puce (1 000 €), appareils de mesure et d'attaque sur la carte à puce (2 000 €), logiciels divers (900 €). **Total** : 3 900 €
Personnel	Un ingénieur de développement HW/SW (10 hommes × mois : 19 800 €), un stagiaire pour réaliser les mesures (5 hommes × mois : 7 800 €). **Total** : 27 600 €
Total	40 000 €

Références

[1] Critères communs. `http://www.commoncriteria.org/`.

[2] Side Channel Laboratory (IAIK, Autriche). `http://www.iaik.tu-graz.ac.at/research/sca-lab/`.

[3] TAMPER Laboratory (Cambridge, Grande-Bretagne). `http://www.cl.cam.ac.uk/Research/Security/tamper/`.

[4] R. Keryell. CryptoPage-1 : vers la fin du piratage informatique ? *SympA'6*, 2000. `http://www.lit.enstb.org/~keryell/publications/ENSTBr_INFO_2000-001/article.pdf`.

[5] J. Jaffe P. Kocher and B. Jun. Differential Power Analysis : Leaking Secrets. *Advances in Cryptology : Proceedings of CRYPTO'99*, 1666 :388–397, 1999.