Action Concertée Incitative CRYPTOLOGIE 2002

I - FICHE D'IDENTITE DU PROJET

Nom du Projet : ***CryptArchi***

Titre du Projet : ***Architectures enfouies pour crypto-systèmes reconfigurables***

Description courte du Projet :

Il s'agit de développer des architectures compactes de calcul dédiées à la cryptographie, ces architectures seront basées sur des modules paramétrables et donc adaptables aux besoins. L'utilisation de composants reconfigurables va permettre l'exécution de plusieurs algorithmes au sein d'un même système. Pour des raisons de sécurité, les différentes parties d'un tel système doivent être incorporées dans un circuit unique. Les circuits reconfigurables actuels atteignent une capacité suffisante pour accueillir un système complet. La mise en œuvre des différents algorithmes nécessite de concevoir leur implantation en adéquation avec une architecture de traitement liée à la structure interne des composants reconfigurables.

Partenaires du Projet	**Laboratoire (pas de sigle)**
Coordinateur	Laboratoire Traitement du Signal et Instrumentation UMR 5516 du CNRS Université Jean Monnet, Saint-Etienne
Autres Partenaires	Laboratoire des Sciences et Matériaux pour l'Electronique et d'Automatique UMR 6602 du CNRS Université Blaise Pascal, Clermont-Ferrand

Action Concertée Incitative CRYPTOLOGIE

II - PRESENTATION DETAILLEE DU PROJET

A - Identification du Coordinateur et des autres partenaires du Projet

A-1 - Coordinateur du Projet

Un unique coordinateur doit être désigné par les partenaires.

Monsieur Prénom : Gérard Nom : Jacquet
Fonction : Maître de conférences
Laboratoire : Traitement du Signal et Instrumentation, UMR CNRS 5516
Adresse : 23, rue Dr. Michelon, 42023 Saint-Etienne
Tél : 04 77 48 50 24 Fax : 04 77 48 50 39 Mail : jacquet@univ-st-etienne.fr

Organisme gestionnaire de l'ACI
Laboratoire : Traitement du Signal et Instrumentation, UMR CNRS 5516

Personne à contacter pour des questions administratives
Monsieur Prénom : Gérard Nom : Jacquet
Fonction : Maître de conférences
Adresse : 23, rue Dr. Michelon, 42023 Saint-Etienne
Tél : 04 77 48 50 24 Fax : 04 77 48 50 39 Mail : jacquet@univ-st-etienne.fr

A-2 - Autres partenaires éventuels du Projet

Partenaire 1

Monsieur Prénom : Jean - Pierre Nom : Derutin
Fonction : Professeur
Laboratoire : LASMEA
Adresse : 24, avenue des Landais 63 117 Aubiere Cedex
Tél : 04 73 40 72 63 Fax : 04 73 40 72 62 Mail : derutin@lasmea.univ-bpclermont.fr

B - Description du projet

B1 – Objectif, contexte et description du projet :

Type d'action : projet d'interface

Nous avons classé ce projet comme un projet d'interface, car il implique des équipes de la communauté des chercheurs en Architecture et Circuits Electroniques qui pour l'instant se retrouvent plutôt autour d'applications concernant les télécommunications, le traitement du signal et des images. La cryptographie pourrait apporter une nouvelle gamme d'applications très intéressantes car différentes d'un point de vue flot de données des applications habituelles.

Objectifs généraux et contexte de la demande

Cette demande d'action concertée constitue pour le laboratoire coordinateur (LTSI) une possibilité de développer un thème de recherche sur les architectures des systèmes de traitement qui pour l'instant est centré sur le traitement des images en temps réel et, via une collaboration industrielle, sur des applications liées au transfert de la voix sur des réseaux de données. L'apparition récente d'une troisième gamme d'applications, liées à la cryptographie, pourrait permettre un développement fort de cet axe si des programmes viennent en soutien.

Cinq enseignants-chercheurs travaillent sur cet axe, deux personnels IATOS/ITA y sont associés pour une part importante de leur temps, deux doctorants complètent l'équipe actuelle. Sur ces personnels, seul un enseignant-chercheur à statut temporaire (PAST étranger) travaille actuellement sur des applications de cryptographie en collaboration avec des laboratoires étrangers (Slovaquie, USA). Cette Action Concertée Incitative servira de déclic au sein du laboratoire TSI pour une co-tutelle de thèse avec une équipe slovaque dès la rentrée 2002, une demande de bourse MESR en 2003. Elle devrait provoquer à terme l'implication de nouveaux collègues enseignants-chercheurs travaillant dans des domaines connexes au sein du groupe. L'évolution de l'environnement de recherche pourrait ainsi permettre de fournir un statut permanent adapté à l'enseignant-chercheur qui a initié ce thème et par-là même constituer un thème de recherche bien positionné au sein du laboratoire.

Plusieurs laboratoires français ayant des équipes travaillant sur l'Architecture et les Circuits Electroniques, sont intéressés par une collaboration avec le LTSI. A l'heure actuelle, un programme de recherche a été défini avec le LASMEA (Clermont-Ferrand) dans lequel cinq personnes travaillent sur le thème des architectures de machines parallèles dédiées, mais plusieurs autres équipes seraient potentiellement intéressées, permettant de mettre en place une véritable dynamique dans le domaine en France.

Enfin, en ce qui concerne le site stéphanois, cette action permettra d'introduire un volet 'cryptographie' dans le cursus d'une Ecole d'Ingénieurs, l'ISTASE, proposant des formations dans le domaine Electronique et Télécommunications. Il est prévu qu'un certain nombre d'investissements soit alors fait par l'école.

Positionnement du projet

Pour des raisons de sécurité, il est préférable de réaliser les fonctions cryptographiques dans des structures matérielles plutôt que de façon logicielle (il est impossible de protéger efficacement les clés confidentielles utilisées par logiciel et stockées dans des endroits peu sûrs comme un disque dur). En plus de l'amélioration de la sécurité, l'implantation de fonctions logiques dans le matériel permet d'augmenter la vitesse du système informatique et de libérer le CPU d'une tâche gourmande. De plus, l'utilisation de circuits reconfigurables permet d'adapter le système cryptographique aux besoins de l'utilisateur et de le faire évoluer.

Il existe aujourd'hui un grand nombre de publications concernant l'implantation de différents algorithmes dans des circuits logiques configurables (CLC), mais très peu d'articles concernant l'architecture d'un système cryptographique complet conçu spécialement pour ce genre de circuits.

Si beaucoup d'efforts ont été concentrés sur les algorithmes de cryptage (à clé symétrique ou asymétrique), la situation est moins favorable pour les fonctions de hachage et encore moins pour la réalisation de générateurs de nombres aléatoires dans des circuits logiques reconfigurables.

Hormis les aspects d'algorithmes et d'implantation de fonctions cryptographiques, la sécurité en ce qui concerne les circuits reconfigurables est traitée de façon insuffisante. Par exemple il semble nécessaire de trouver un moyen de générer les clés confidentielles à l'intérieur du circuit logique, ceci de préférence avec un véritable générateur de nombres aléatoires. Le principe de génération de nombres aléatoires de bonne qualité à l'intérieur d'un circuit logique ne semble pas réalisé à ce jour.

Or, le placement d'un tel générateur en dehors du circuit ne permettrait pas de s'affranchir de manipulations éventuelles des nombres générés, qui constituent la base de futures données confidentielles. Il paraît également important d'estimer les possibilités d'attaques externes vis-à-vis du circuits (side-channel attacks) et de les contrer. Il serait intéressant d'évaluer les possibilités d'utiliser les différentes broches d'alimentation pour obtenir une information sur les clés confidentielles et sur la localisation des différentes fonctions à l'intérieur du circuit.

Ce projet a été classé comme projet d'interface, puisqu'il doit proposer des solutions aux problèmes électroniques (conception et réalisation d'une architecture et/ou d'une fonction cryptographique, etc.) en optimisant et en modifiant les algorithmes cryptographiques et en veillant sur les paramètres de sécurité (vulnérabilité, etc.) de la solution proposée.

Situation actuelle en France :

Il ne semble pas y avoir à ce jour en France d'équipe de recherche qui soit focalisée sur l'ensemble des problèmes concernant l'implantation de fonctions cryptographiques dans des circuits logiques reconfigurables et les conséquences d'une telle implantation (sécurité, vulnérabilité…).

Collaboration avec d'autres laboratoires étrangers

Grâce aux précédents travaux de Mr Fischer, des contacts ont été établi avec des laboratoires étrangers travaillant dans ces domaines. Notamment le « Department of electronics and multimedia communications », Technical University of Kosice (TUKE) en Slovaquie, propose sa participation. Ce laboratoire est spécialiste en traitement du signal et en sécurité des systèmes de communication. Mr Milos Drutarovsky, qui a déjà participé à plusieurs publications communes sur le sujet avec Mr Fischer, est intéressé par une collaboration sur ce projet.

De même, Mr Kris Gaj, responsable du laboratoire « Cryptography and Network-Security Implementations », Department of Electrical and Computer Engineering George Mason University (GMU) aux USA s'est proposé pour une collaboration sur ce sujet. Il est lui même spécialiste d'implantation de fonctions cryptographiques dans les CLC de type FPGA.

Ces deux collaborations pourraient être profitables au projet et enrichissantes pour tous. Une rencontre avec les personnes citées ci-dessus, ainsi que leurs collègues travaillant sur les mêmes domaines, à des fin consultatives, serait souhaitable.

Objectifs scientifiques :

1. Développer les architectures des systèmes cryptographiques performants et souples. Evaluer les possibilités d'une conception mixte matériel/logiciel (hadware/software co-design) avec un ou plusieurs multiprocesseurs incorporés, ceci pour différentes familles de circuits logiques configurables (CLC) - CPLD, FPGA. Estimer les possibilités de paralléliser les traitements dans le matériel (structures pipeline) et dans le logiciel (structures multiprocesseur).
2. Développer des fonctions cryptographiques paramétrables adaptées à l'implantation dans des circuits logiques reconfigurables. Les fonctions de base utilisées pour assurer la confidentialité, l'intégrité de données et l'authenticité, doivent être sélectionnées parmi celles proposées dans le cadre de programmes AES et NESSIE. Adapter les algorithmes existants à l'implantation dans les CLC pour obtenir une meilleure performance (rapport surface utilisée / vitesse atteinte) et comparer leur implantation dans différentes familles de CLC – CPLD et FPGA.
3. Mesurer la sécurité et la performance des systèmes proposés. Evaluer les possibilités d'attaques externes (side-channel attacks) et chercher un moyen d'augmenter la résistance des systèmes reconfigurables contre ces attaques. Sonder la consommation du circuit en cours d'utilisation (pendant le cryptage), pour voir s'il est possible d'en tirer des informations sur les informations confidentielles. S'il s'avère possible d'extraire une information pertinente par ce moyen, il sera nécessaire de modifier l'algorithme ou l'implantation pour cacher cette information.

Caractère innovant :

- L'expertise générale et approfondie d'utilisation des CLC en cryptographie n'a pas encore été faite.
- Les architectures mixtes avec matériel et logiciel incorporés dans le même circuit ont été peu évaluées pour les applications cryptographiques.
- Certaines fonctions cryptographiques (par exemple les générateurs des nombres aléatoires) n'ont pas été proposées pour les CLC.
- La résistance des CLC et des fonctions cryptographiques implantées contre les attaques externes n'a pas été examinée jusqu'ici.

Tâches à réaliser dans le cadre de différents objectifs :

Le développement d'architectures spécifiques dans différentes familles de CLC (FPGA, CPLD) est la tâche de fond qui occupera les différents partenaires toute la durée du projet. Le TSI aura pour mission de concevoir et de tester plusieurs types d'architectures, alors que le LASMEA s'intéressera plus particulièrement à la parallélisation des fonctions.

Pendant la première année, plusieurs algorithmes seront testés et optimisés pour chacune des cibles retenues.

La seconde année sera plutôt consacrée à l'aspect sécurité : évaluation de la robustesse des systèmes développés et de leur résistance aux attaques, et éventuellement amélioration de ces paramètres.

L'organisation d'un séminaire regroupant tous les partenaires impliqués dans le projet est également à prévoir au moins une fois par ans, ainsi que la participation à des conférences internationales.

1. Les tâches à réaliser dans le cadre du premier objectif

A) Développer et évaluer les architecture enfouis qui seront

- adaptées à l'implantation dans les CLC
- évolutives (pour modifier/ajouter facilement les algorithmes sélectionnés dans le cadre du programme NESSIE).

Personnes concernés : les personnes du LTSI impliquées dans le projet

B) Evaluer les différents types d'interface entre le processeur et la logique enfouie du point de vue vitesse et surface utilisée. Sélectionner l'interface qui sera utilisée ultérieurement.
Personnes concernées : M. Fischer, LTSI

C) Tester l'aspect parallélisme pour les différents algorithmes sur une machine parallèle multi-power G4.
Personnes concernés : JP. Dérutin et J. Serot , LASMEA

D) Chercher le rapport optimal entre l'utilisation de la surface interne par le logiciel (ressources mémoire) et par le matériel (processeur, coprocesseur, logique de contrôle, etc.)
Personnes concernées : M. Fischer, LTSI, TUKE

2. Les tâches à réaliser dans le cadre du deuxième objectif

A) Choisir les primitives cryptographiques à implanter dans le système enfoui, ceci parmi les algorithmes sélectionnés dans les programmes AES et NESSIE.
Personnes concernées : LTSI, TUKE, GMU

B) Implémenter les algorithmes sélectionnés dans le cadre de la tâche 2A.
Personnes concernées : LTSI, TUKE

C) Proposer des versions parallélisées pour les algorithmes susceptibles de l'être.
Personnes concernées : : JP. Dérutin et J. Serot , LASMEA

3. Les tâches à réaliser dans le cadre du troisième objectif

A) Evaluer la sécurité et la performance des architectures proposées.
Personnes concernées : LTSI, TUKE, GMU

B) Tester la résistance des systèmes proposés contre les attaques externes.
Personnes concernées : LTSI, TUKE

C) Expertiser différentes familles de CLC pour leur utilisation dans les applications cryptographiques.
Personnes concernées : LTSI, TUKE, GMU

4. Les tâches supplémentaires

A) Organisation d'un séminaire réunissant tous les partenaires en fin de chaque année.
Personnes concernées : LTSI, LASMEA, TUKE, GMU

Planning :

	Année 2003				Année 2004			
tâche	tr1	tr2	tr3	tr4	tr1	tr2	tr3	tr4
1A								
1 B								
1 C								
1 D								
2 A								
2 B								
2 C								
3 A								
3 B								
3 C								
4 A								

Risques scientifiques

Par rapport à l'objectif premier qui est la mise au point et l'implantation d'architectures mixtes matériel et logiciel au sein d'un même circuit logique, les risques qui peuvent être encourus seraient d'aboutir à des systèmes difficilement exploitables en ce qui concerne le rapport d'occupation de ressources logiques par rapport à la capacité mémoire occupée par le programme. Dans le cas de l'utilisation excessive de ressources mémoire, celle-ci pourrait par exemple être réduite par un « glissement » de quelques tâches du processeur vers le matériel (coprocesseur) pour obtenir une solution plus équilibrée.

Un autre paramètre à suivre est le rapport vitesse / surface utilisée. La solution plus souple, utilisant les processeurs enfouis, ne garanti pas obligatoirement son optimisation.

En ce qui concerne l'implantation de fonctions cryptographiques (fonctions de cryptage à clé symétrique et asymétrique, fonction de hachage, gestion de clés confidentielles, etc.), les risques scientifiques sont liés à la difficulté d'implanter l'ensemble de ces fonctions de façon optimale dans un seul circuit. De plus, pour la génération de nombres véritablement aléatoires (et non pas pseudo-aléatoires) la situation parait encore plus défavorable : il faut trouver à l'intérieur du circuit exclusivement logique, une source analogique aléatoire exploitable. La réussite dans la réalisation de cette fonction dépend de la structure interne de la famille de CLC et de la technologie utilisée par le fabriquant de ce gendre de circuits.

Les risques les plus importants se situent autour du troisième objectif, qui est d'estimer la sécurité d'implantation de nos systèmes. Pour cela, il est nécessaire d'être capable de mesurer des phénomènes physiques rapides et de faible amplitude, et d'exploiter les résultats de ces mesures de façon statistique. Au cas où une information relevante sera possible de tirer de cette mesure par une exploitation statistique, il sera nécessaire de modifier la structure interne du circuit et/ou la méthode (fonction) cryptographique pour éviter l'échappement d'une information confidentielle.

B2 – Organisation :

Nom	Prénom	Laboratoire ou équipe de rattachement	Poste statutaire	% du temps de recherche consacré au projet
Jacquet	Gérard	TSI	MC	20 %
Fischer	Viktor	TSI	PAST	100 %
Bochard	Nathalie	TSI	IE CNRS	40 %
Celle	Frédéric	TSI	AI MESR	10 %
A recruter		TSI/TUKE	Doctorant	100 %
Dérutin	Jean-Pierre	LASMEA	Pr	20 %
Serot	Jocelyin	LASMEA	MC	20 %

B3 – Références :

[1] J. Dubois, G. Jacquet, G. Motyl, V. Fischer, R. Fouquet, *System for real time motion measurement*. CD ROM : Education and Research Conference Proceedings 2000\Formal Presentations\5. Video & Image Processing\System for Real Time Motion Measurement.pdf, Paris, Sept. 2000.

[2] J. Dubois, G. Jacquet, V. Fischer, G. Motyl and R. Fouquet, *Parallel Structure for Physical Measurement by Image Processing.* Proceedings of DCIS 2000, Montpellier, Nov. 2000, pp. 444 - 449.

[3] J. Dubois, G. Jacquet, G. Motyl, F. Celle and V. Fischer, *Round-About: une architecture de traitement d'images pour la mesure en temps réel de paramètres physiques*, Proceedings of the 18th Symphosium GRETSI on Signal and Image Processing (on CD) , Toulouse, Sept 10-13, 2001.

[3] V. Fischer, *Realisation of the RIJNDAEL Cipher in Field Programmable Devices.* Proceedings of DCIS 2000, Montpellier, Nov. 2000, pp. 312 - 317.

[4] V. Fischer, J. Dubois, *Flexible Didactic Card with Embedded Processor*. Proceedings of DCIS 2000, Montpellier, Nov. 2000, pp. 392 - 396.

[5] V. Fischer, M. Drutarovský, *Two Methods of Rijndael Implementation in Reconfigurable Hardware*, Cryptographic Hardware and Embedded Systems – CHES'2001, LNCS 2162 (2001), pp. 77-92.

[6] V. Fischer, M. Drutarovský, *Scalable RSA Processor in Reconfigurable Hardware - a SoC Building Block*, DCIS 2001 Conference, pp. 327-332, Porto, Nov. 2001.

[7] Miloš Drutarovský, Viktor Fischer, *Implementation of Scalable Montgomery Multiplication Coprocessor in Altera Reconfigurable Hardware*, International Conference on Signal Processing and Telecommunications, Kosice, Slovakia, Nov. 2001, pp. 132-135.

[8] J. Sérot. The SKiPPER project : skeletons for parallel image processing. MiniSymposium on Advanced Programming Environments for Parallel and Distributed Computing, ParCo Intl. conf., 4-7 Sep 2001.

[9] J. Sérot, D. Ginhac, R. Chapuis, and J.P. Dérutin. Fast prototyping of parallel vision applications using functional skeletons. *Journal of Machine Vision and Applications*, 12(6):271-290, June 2001.

10] J. Sérot R. Coudarcher and J.P. Dérutin. Implementation of a skeleton-based parallel programming environment supporting arbitrary nesting. In F. Mueller, editor, *6th Int. Workshop on High-Level Parallel Programming Models and Supportive Environments*, volume 2026 of *LNCS*, pages 189-196, San-Francisco, CA, USA, Apr 2001. Springer.

[11] J. Sérot, D. Ginhac, and J.P. Dérutin. SKiPPER: a skeleton-based parallel programming environment for real-time image processing applications. In V. Malyshkin, editor, *5th International Conference on Parallel Computing Technologies (PaCT-99)*, volume 1662 of *LNCS*, pages 296-305. Springer, 6-10 September 1999.

B4 – Moyens financiers demandés dans le cadre de l'ACI :

Pour venir compléter les équipements dont dispose le laboratoire TSI (FPGA Advantage de Mentor Graphics et les outils de développement spécifiques à ALTERA : MaxPlusII et QuartusII), nous aurons besoin de nous procurer un outil de développement pour circuits XILINX qui nous permettra de vérifier l'adéquation des différentes familles de CLC à l'application cryptographique (reconfiguration partielle, consommation, interface JTAG, vulnérabilité aux attaques externes).

Il nous faudra également du matériel informatique performant pour pouvoir développer sur des circuits de grande capacité.

Pour le test des algorithmes nous envisageons d'investir dans des cartes de développement performantes proposées par les fabricants de CLC.

Le LASMEA quant à lui envisage de s'équiper d'une carte ALTERA APEX II - 1500 et de l'environnement de développement Excalibur, ainsi que de réactualiser les cartes processeurs G4 de la machine parallèle OSSIAN.