# 1 Résumé

La carte à puce est depuis 10 ans moteur d'innovation en cryptographie à clef publique. Dans Eurocrypt'88, $C^*$, un nouveau cryptosystème à clef publique, basé sur des polynômes multivariables de degré 2 est proposé par MATSUMOTO et IMAI. S'il avait été solide, il aurait été idéal pour la carte à puce. Cependant, il est cryptanalysé par Jacques PATARIN dans Crypto'95. Dans ce rapport, nous étudions la sécurité des systèmes similaires, dans le contexte précis des applications dans des cartes à puce.

Nous montrons une attaque surprenante sur un système appelé $D^*$, cryptanalysé depuis peu par une attaque indépendante. Notre méthode permet même d'obtenir la clef secrète. On ne savait le faire jusqu'ici pour aucun cryptosystème de la famille. Ce problème est en toute généralité appelé IP. Nous présenterons quatre nouvelles méthodes pour le résoudre, dont la meilleure est en $\mathcal{O}(q^{n/2})$. Le meilleure attaque connue jusque là était en $\mathcal{O}(q^{n\sqrt{n}})$. Cela permet d'espérer de trouver de nouveaux algorithmes pour la multiplication rapide de matrices.

Nous montrons qu'un autre système HM, basé sur les matrices, proposé en 1985 n'est pas sûr, et nous étudions comment le réparer. Nous montrons aussi un certain nombre de propriétés génériques des cryptosystèmes étudiés qui mènent à des nouvelles attaques. En particulier, nous montrons comment attaquer "Scotch". Nous étudions avec soin des conditions d'utilisation des boîtes $S$ dans des nouveaux cryptosystèmes.

# 2 Abstract

Smart card implementations has been, for the last 10 years, a major inducement for innovation in public key cryptography. In EUROCRYPT'88 , the $C^*$, a new, multivariate quadratic equation based, public key cryptosystem is proposed by MATSUMOTO and IMAI. Strikingly simple, it requires amazingly little computation. Jacques Patarin broke it in Crypto'95. In this work we have been studying similar ideas within the framework of possible smart card applications.

We show a surprising attack of a cryptosystem called $D^*$, recently known to be independently broken. Yet our approach seems more powerful and allows us to find the whole secret key, which hasn't been done for any cryptosystem of the kind. This an exemple of a general problem called IP. We introduce four new solving techniques, the best in $\mathcal{O}(q^{n/2})$. The best complexity so far was $\mathcal{O}(q^{n\sqrt{n}})$. It gives hope to find new better fast matrix multiplication algorithms.

We also show that another matrices-based system HM, proposed in 1985, is not secure and we inquire how to repair it. We point out several generic properties of all studied schemes which suggest new attacks. We show how to attack "Scotch" and we have determined precise conditions of use of $S$- boxes in such schemes and their security.