Trois chercheurs de l'Université du Michigan, A. Pellegrini, V. Bertacco et T. Austin, ont monté une attaque par faute sur RSA 1024 bits, qui semble très efficace. L'annonce est faite ici . On trouvera une copie de l'article correspondant : "
Fault-Based Attack of RSA Authentication"
par Andrea Pellegrini, Valeria Bertacco and Todd Austin sur
la page web de Valeria Bertacco
.