http://uobabylon.edu.iq/media/press.aspx?mid=49201

دراسة في كلية تكنولوجيا المعلومات تبحث الهجوم الجبري على مولد الربط غير الخطي

بحثت دراسة في كلية تكنولوجيا المعلومات أعدها الدكتور ستار بدر سدخان، والباحثة رفيف محمد حمزة الخفاجي (الهجوم الجبري على مولد الربط غير الخطي).تناولت الدراسة التشفير الانسيابي الذي يلعب دوراً هاماً في علم التشفير، وبينت إن المشكلة الأساسية في نظام التشفير الانسيابي هو صعوبة توليد سلسلة (متتالية) ثنائية طويلة لا يمكن التبوء بها (keystream) من سلسلة (مفتاح) صغيرة.
;nbsp;   &
وأوضحت الدراسة أنه يجب أن تكون السلسلة المتولدة ذات طول دوري كبير وخصائص إحصائية جيدة، ويعتبر مولد النبضة (clock control) أحد المولدات المستخدمة في توليد مثل هذه السلاسل, حيث أنه يعتمد على المسجلات ذات التغذية الخطية المرتدة (LFSR) لكن مع الحركة غير المنتظمة للمسجلات التي يتكون منها، ويعتبر مولد (LILI) أحد مولدات (clock control) المعتمدة على الحركة غير المنتظمة لمولد الترشيح، ويمكن استخدام هذه الفكرة مع تبديل مولد الترشيح (filtering) بمولد التوحيد (combiner)، وإن التشفير الانسيابي كأحد أوليات علم التشفير الأخرى يمكن إن يتعرض إلى العديد من أنواع الهجوم . وتهدف الدراسة إلى كيفية تصنيف أنواع الهجوم بالاعتماد على المعلومات المباحة للمهاجم، أو الطريقة المستخدمة للهجوم، أو ما هو الهدف من الهجوم.واقترحت الدراسة مولد (clock control) يعتمد على مولد التوحيد (combiner) بدلا من مولد الترشيح (filtering) الذي يستخدم في المولد (LILI) التقليدي وذلك لزيادة تعقيد المولد.واستنتجت الدراسة أن تطبيق الهجوم الجبري على المولدين أثبت نجاحه, وإن مقاومة النظام التقليدي أكثر من مقاومة النظام المقترح، وهذا يعني إمكانية نجاح الهجوم الجبري حتى في حالة زيادة تعقيد المولد .

رافع عبد القادر