"On Some Symmetric Lightweight Cryptographic Designs" — En Populärvetenskaplig Sammanfattning

Martin Ågren

Inst. för Elektro- och Informationsteknik, Lunds Universitet,
Box 118, 221 00 Lund
martin.agren@eit.lth.se

Kryptering finns på många ställen i samhället, även om vi inte alltid är medvetna om det: kreditkorten vi använder i automater och butiker; dosorna vi använder för att uträtta bankärenden över Internet; bankernas datorer som kommunicerar med varandra för att flytta stora belopp varje minut; mobiltelefonerna och basstationerna som skickar samtal och SMS mellan varandra; RFID-taggar, som kan avläsas med hjälp av radiovågor och som spås ta över efter de optiska streckkoderna i allt fler sammanhang; BankID:t vi använder när vi deklarerar över Internet; listan kan göras lång.

Flera av exemplen ovan har det gemensamt att det handlar om en liten enhet, till exempel ett litet chip, en liten telefon eller en liten dosa, som måste utföra de kryptografiska beräkningarna. Eftersom dessa små enheter ofta är batteristyrda, eller över huvud taget inte innehåller något batteri utan drivs helt och hållet av radiovågor, är det av stor vikt att krypteringen är så energieffektiv som möjligt. (Det kan även tänkas att telefonen blir lättare att sälja om krypteringen använder lite ström, så att desto mer kan förbrukas av färgskärmen och högtalaren.)

På senare år har flera "*lättviktskrypton*" presenterats som är avsedda just för sådana här lättviktsapplikationer. Man kan säga att det är ganska rättframt att konstruera en säker krypteringsalgoritm, men desto svårare att skapa en *effektiv* algoritm som ändå inte tummar på säkerheten. Dessa lättviktskrypton balanserar medvetet väldigt nära gränsen för hur effektiv man kan vara utan att brista i säkerheten.

Kortfattat kan man säga att en krypteringsalgoritm är säker om den beter sig på ett slumpmässigt sätt. När man stoppar in en klartext och en nyckel och får ut en kryptotext, ska den se "fullkomligt slumpmässig ut". Till exempel ska en liten ändring i klartexten och/eller nyckeln orsaka en stor ändring i kryptotexten.

Den här avhandlingen har undersökt några olika lättviktskrypton, nämligen BEAN, KTANTAN och PRINTcipher, samt presenterat några nya algoritmer.

BEAN visar sig mycket sårbart mot vad man kan kalla igenkänningsattacker (eng. "distinginguishing attacks"). Genom att observera ungefär 6 KB kryptotext (exempelvis en krypterad version av den här texten) kan man avgöra huruvida krypteringen gjordes med hjälp av BEAN eller någon annan algoritm — man kan "känna igen" BEAN.

KTANTAN visar sig ha vissa problem i det så kallade nyckelschemat. Detta är delvis redan känt, men avhandlingen visar att omfattningen är större än vad

som var känt tidigare. Om man tillåter en angripare att få två krypteringar av en klartext, en som svarar mot den riktiga, hemliga nyckeln och en som svarar mot en nyckel som har ändrats lite, så kan angriparen hitta den hemliga nyckeln på en halv *minut* med hjälp av en modern dator, när det borde ta väldigt många *år* om KTANTAN var helt säkert. Det är visserligen svårt att tänka sig att en sådan här relaterad-nyckel-attack (eng. "related-key attack") någonsin skulle gå att genomföra, men KTANTAN är skapat för att motstå dem och därför är resultatet i avhandlingen ändå anmärkningsvärt.

PRINTcipher visar sig vara olika sårbar för så kallad lineär kryptanalys (eng. "linear cryptanalysis") beroende på valet av nyckel. Den statistiska egenskap som utnyttjas i attacken visar sig dessutom kunna observeras flera gånger i varje par av klartext–krypotext, vilket möjliggör en starkare attack.

PRINTcipher har även analyserats av Leander m.fl., som visade hur algoritmen för vissa nycklar bevarade information om klartexten i kryptotexten. Man visade även hur detta relaterar till lineär kryptanalys. Avhandlingen studerar detta närmare och visar med hjälp av några nya resultat kring lineär kryptanalys precis vad som händer "inuti" PRINTcipher och varför det händer som Leander m.fl. visade.

Vid sidan av kryptering, som kan sägas handla om att hemlighålla information, har även autentisering undersökts, det vill säga hur mottagaren av ett (möjligen krypterat) meddelande kan försäkra sig om att det inte ändrats på vägen från avsändaren. Avhandlingen föreslår en ny typ av konstruktion för autentisering, som förefaller vara lämplig att använda tillsammans med lättviktskrypton.

Avhandlingen föreslår även en krypteringsalgoritm med inbyggt stöd för autentisering. Den föreslagna konstruktionen, Grain-128a, är den senaste medlemmen i kryptofamiljen Grain och tycks vara väldigt lämplig i lättviktsapplikationer.

Sammanfattningsvis har avhandlingen visat på problem i några av de algoritmer som föreslagits för lättviktsapplikationer, men även breddat förståelsen kring dessa problem. Förhoppningsvis kan innehållet i avhandlingen utgöra en grund för framtida lättviktsalgoritmer i telefoner, bankdosor och RFID-taggar.