

# Framtidssäkrat internetsurfande - både snabbt och tryggt

Populärvetenskaplig sammanfattning av examensarbete

FÖRFATTARE Matilda Backendal

HANDLEDARE Felix Günther (UCSD) och Thomas Johansson (LTH)

EXAMENSARBETE Puncturable Symmetric KEMs for Forward-Secret 0-RTT Key Exchange

---

**Integritet på nätet eller snabb uppkoppling? Med dagens krypteringsmetoder är det antingen eller, men i framtiden behöver vi kanske inte kompromissa.**

I takt med att samhället digitaliseras flyttas alltmer kommunikation till internet, vilket i många fall gör livet smidigare. Samtidigt blir vi mer sårbara då data som skickas över nätet eller lagras online riskerar att läcka ut och bli allmänt känd. För att värna om vår integritet och säkerhet vidtas åtgärder för att dölja information som skickas via nätet, men dessa insatser är tidskrävande och innebär extra överföringar vilket gör uppkopplingen långsammare.

Mer specifikt skyddas internetanslutningar till webbadresser som inleds med 'https' idag av kryptering som gör kommunikationen oläslig för alla utomstående. Utan tillgång till nycklar som "läser upp" och dechiffrerar de krypterade meddelandena är de inget mer än rappakalja. För att de kommunicerande parterna ska kunna ta del av innehållet krävs därför att de utbyter krypteringsnycklar. Detta sker i början av uppkopplingen för att se till att krypteringen i varje anslutning är oberoende av tidigare sessioner. Man kan säga att nycklarna är som engångsartiklar. De förhandlas fram, används i en session och slängs sedan. Själva utbytet, när parterna kommer överens om nycklarna, bromsar uppkopplingen och gör att anslutningen upplevs som långsam. Men det finns snabbara sätt.

**Nyligen lanserades** en snabbuppkopplingsfunktion som gör det möjligt att återansluta utan det inledande nyckelutbytet. Förenklat kan man säga att om de kommunicerande parterna har varit i kontakt tidigare och redan delar nycklar från en tidigare session, så kan dessa återanvändas för att kryptera även framtida anslutningar. Effekten blir en markant prestandaökning.

Tyvärr ger den nya funktionen lägre säkerhetsgarantier än vid ett fullt nyckelutbyte. Detta eftersom återanvändningen av kryptografiskt material potentiellt leder till att alla sessioner där samma nycklar har använts blir oskyddade om nycklarna läcker ut. Det finns naturligtvis alltid en risk att någon knäcker krypteringen eller kommer över de nycklar som används, men då engångsnycklar an-

vänds leder det bara till att kommunikationen i den pågående sessionen blir synlig för förövaren. Om nycklarna däremot har använts till flera sessioner, riskerar alla dessa att bli oskyddade.

**I det här arbetet** undersöks möjligheten att behålla den snabba uppkopplingen som den nya funktionen ger, men utan att behöva kompromissa om säkerheten. Idén bygger på ett smart sätt att återanvända nycklar. Istället för att använda exakt samma nyckel till flera sessioner uppdateras nyckeln mellan varven, så att tidigare sessioners kommunikation inte går att dekryptera om den nya, förändrade nyckeln läcker ut. Operationen kallas för punktering, och man kan föreställa sig att förmågan att dekryptera vissa meddelanden försvinner när nyckeln punkteras, ungefär som när en biljett klipps efter användning. Den går fortfarande att använda till framtida sessioner, men avslutad kommunikation som nyckeln har "punkterats på" är lika oläsbar med den punkterade nyckeln som utan den.

Det här projektet har gått ut på att skapa en modell som visar hur punkterade nycklar skulle kunna användas för att ge både snabb uppkoppling och den önskade säkerheten. Modellen består av en ny matematisk abstraktion som fångar hur den nya funktionen tillåter snabba uppkopplingar. Den innehåller också en påbyggnad som beskriver hur punktering kan användas för högre säkerhetsgarantier. Modellen visar att det i teorin är möjligt att genom punktering uppnå både hög säkerhet och prestanda, men att det finns vissa nackdelar med tillvägagångssättet. Framförallt är det problematiskt att de punkterade nycklarna kräver mer lagringsutrymme än vanliga nycklar, vilket i vissa fall kan vara ett hinder. I arbetet har det därför också undersökts hur ordningsföljden av återanslutna sessioner skulle kunna utnyttjas för att hålla ned storleken på de punkterade nycklarna. Detta genom att designa algoritmer så att det vid normal användning skapas platseffektiva "punkteringsmönster". Studien visar att det finns potential hos förslaget. För att avgöra om idén med punkterbara nycklar är värd att lansera i stor skala krävs dock fortsatta undersökningar där konstruktioner implementeras och testas på verkliga scenarion.