Decryption Failure Attacks on Post-Quantum Cryptography

Nilsson, Alexander

2023

Document Version:
Publisher's PDF, also known as Version of record

Populärvetenskaplig sammanfattning

Kvantdatorer bedöms kunna ha kapacitet att knäcka kryptering, även om risken ligger ett antal utvecklingsår framåt i tiden. Det är ju bra för oss som bryr oss om säkerhet, men det tar lång tid att bl.a. designa, utvärdera, standardisera, implementera och distribuera nya kryptalgoritmer. Därför är det av största vikt att det arbetet startar i god tid.

En säker krypteringsalgoritm utgår från en solid teoretisk säkerhetsgrund, men vid implementation i mjukvara och/eller hårdvara riskerar man introduktion av nya sårbarheter. Algoritmens inre tillstånd kan nämligen påverkas eller läckas genom olika attackteknikер.

Sidokanalsattacker (eng. side-channel attacks, SCA) är en gren inom kryptanalys och är ett viktigt ben som denna avhandling vilar på. Vid SCA kan man mäta t.ex. tidsvariationer för att nyttja beroenden mellan indata och tillstånd, eller utläsa olika exekveringsvägar inom algoritmen. Detta är ett väldigt kraftfullt verktyg för en angripare, då en upptäckt sårbarhet har god chans att kunna nyttjas över nätverk, och utan fysisk tillgång till det angripna målet. Vissa tidsvariationer har sitt ursprung i algoritmernas uppbyggnad, d.v.s. beroende på hur den hemliga nyckeln ser ut kommer beräkningar utföras på olika sätt. Andra tidsvariationer uppstår vid översättningen från teori till maskinkod.

SCA kan även orsakas av strömförbrukningsvariationer eller variationer av elektromagnetisk strålning. I dessa fall krävs fysisk tillgång för att kunna utföra mätningar. Många användarfall placerar hårdvara som t.ex. smarta kort eller Internet-Of-Things (IOT) i exponerade miljöer och dessa bör därför vara skyddade, även mot sådana fysiska attacker.

Denna avhandling handlar i huvudsak om hur insamling av dekrypteringsfel kan ge en angripare tillräckligt med information för att knäcka antingen den hemliga nyckeln eller ett hemligt meddelande. För många krypteringsalgoritmer finns det nämligen en gemensam egenskap. De har alla en osannolik, men ändå större än noll, risk för att dekryptering skall misslyckas för korrekt krypterade meddelanden. Kända krypteringsalgoritmer har valt parametrar så att risken är minimal, men som forskningen i denna avhandling visar, kan denna egenskap fortfarande orsaka problem, i vissa fall.

Denna avhandling fokuserar på skärningspunkten av implementationsaspekter, kryptanalys, kodningsteori och lite gitter-baserad kryptografi, enligt nedanstående beskrivningar.

Implementationsaspekter syftar till forskning på upptäckta brister och sidokanalsläckage i mjukvaruimplementationerna av kryptalgoritmer. Forskningen inkluderar även en alternativ implementation av en specifik del av en krypteringsalgoritm.

Kryptanalys innebär försök att förbättra förståelsen för nästa generation av kryptalgoritmer. I några fall upptäckte vi nya sårbarheter i källkoden, i andra fall publicerade vi nya strategier för att förbättra redan existerande attacker. Här återfinns även nya teoretiska resultat kring den praktiska säkerhetsnivån för några av nästa generations krypteringsalgoritmer, i relation till dekrypteringsfel, som nämnts ovan.

Kodningsteori relaterar till teori kring felrättande koder, antingen som ett analytiskt verktyg, eller för att de berör kodbaserade krypteringsalgoritmer. Felrättande koder används framförallt för att skicka och ta emot signaler över olika medium, men kan även användas inom kryptografi då felkorrigering av slumpmässiga och ostrukturerade koder är ett beräkningsmässigt svårt problem. Detta kan tillämpas som en god teoretisk grund för säkerheten för vissa av nästa generationens krypteringsalgoritmer.

Gitter-baserad kryptering är en viktig del av denna avhandling då några algoritmer av denna typ utsätts för varierande grad av granskning. Gitter (eng. Lattice) kan liknas vid N-dimensionella koordinatsystem med endast heltalskoordinater, där N i kryptosammanhang är ett stort tal. Kring dessa matematiska konstruktioner kretsar ett antal problem, vars lösningar är mycket tunga att beräkna. Detta ligger till grunden för säkerheten för många av nästa generations krypteringsalgoritmer.

"Attacker blir bara bättre, inte sämre" är en välkänd truism inom fältet kryptanalys. Detta är ett viktigt forskningsområde eftersom den praktiska tillämparheten ofta används som en måttstock över hur mycket kraft som skall spenderas på att förebygga och mitigera attacker. Nya, tidigare okända, attacker fyller samma syfte, fast med något större genomslag i det kryptanalytiska forskningsområdet. Det beror naturligtvis på att implementationsproblem bara kan fixas om de är kända. I denna avhandling gav vi också ett förslag till en alternativ subkomponent till en redan känd kryptalgoritm. Detta ifrågasätter "status quo" och driver innovation, även om det specifika alternativet i fråga inte har kommit till någon vidare användning. Slutligen, finner vi även forskningsbidrag som ligger mer åt det teoretiska hållet och medan det är användbart i sig själv så bidrar det även rent generellt till den större massan av kryptanalytisk kunskap. Detta höjer förtroendet för den viktiga säkerhetsutvärderingen av nästa generation av kvantdatorsäkra krypteringsalgoritmer.