Post-quantum security of cryptographic transformations in the random oracle model

Huang, Y.

Samenvatting

Een cryptografisch algoritme wordt doorgaans in meerdere stappen ontworpen: eerst wordt een eenvoudiger (maar zwakker) algoritme opgesteld, en dit wordt later aangepast tot een sterker en geavanceerder algoritme. In sommige stappen is het gebruikelijk om een generieke transformatie toe te passen die niet is afgestemd op het specifieke algoritme in kwestie. Het doel van het dit proefschrift is om de veiligheid van dergelijke transformaties rigoreuze en bewijsbaar te vaststellen, in de context van post-quantumcryptografie (PQC). De meeste van onze resultaten zijn verkregen in een geïdealiseerde setting die bekend staat als het *random oracle model* (ROM), waarin cryptografische hashfuncties (of sommige delen hiervan) worden gemodelleerd als een willekeurige functie — een random oracle — die zowel door de constructie als door de aanvallers kan worden geraadpleegd. Dit staat in contrast met het *plain model*, wat niet zo'n dergelijke idealisering kent.

In Hoofdstuk 3 bestuderen we de ontwerpprincipes van Fiat-Shamir with aborts (FSwA) en hash-and-sign with retry/aborts (HSwA). Deze transformaties zijn populair bij post-quantum digitale handtekeningalgoritmes, maar de analyse blijkt lastig te zijn. Zoals beschreven in het hoofdstuk, hebben alle eerdere veiligheidsanalyses van FSwA dezelfde subtiele maar cruciale fout, die ook terugkomt in HSwA. Deze fout maakt eerdere veiligheidsbewijzen van alle algoritmes die op FSwA zijn gebaseerd ongeldig, waaronder Dilithium, een van de standaarden die zijn geselecteerd door het Amerikaanse National Institute of Standards and Technology (NIST). We herstellen de veiligheid van FSwA en HSwA handtekeningenalgoritmes door nieuwe, gecorrigeerde veiligheidsbewijzen te leveren in een uniform kader dat beide omvat.

Onze analyses hebben betrekking op zowel klassieke als quantumaanvallen. De technische kern hiervan ligt in een hybride rijtje, waarin het random oracle wordt hergeprogrammeerd. We stellen met name dat, als we de waarden van een random oracle op een bepaalde manier herprogrammeren en vervolgens een deel van die herprogrammering ongedaan maken, een aanvaller in deze reeks wijzigingen aan het random oracle waarschijnlijk geen verschil zal merken. Voor een aanvaller die maximaal q_H quantumvragen aan het random oracle mag stellen en q_S klassieke vragen aan een onderteken orakel, gaat dit in eerste instantie gepaard met een additief veiligheidsverlies van de orde $O(q_H\sqrt{q_S\epsilon})$,

waarbij ϵ een algoritme-afhankelijke parameter is die dicht bij nul ligt. Later verbeteren we dit tot $O(q_S\sqrt{q_H\epsilon})$, via een meer geavanceerd hybride rijtje. Deze verbetering komt kwantitatief overeen met de meest geavanceerde bovengrenzen in het beter begrepen geval van de Fiat-Shamir transformatie (*zonder* aborts). Hoewel het nog onduidelijk is of onze grenzen optimaal zijn, zouden verdere verbeteringen (voor zover zij bestaan) ook doorgevoerd kunnen worden in de beter begrepen setting zonder aborts.

In Hoofdstuk 4 bestuderen we de BUFF transformatie, een transformatie voor handtekeningenalgoritmes die als doel heeft om aanvullende beveiligingseigenschappen te bieden naast de standaard onvervalsbaarheid. We tonen aan dat een van deze eigenschappen, namelijk non-resignability (NR), subtieler is dan eerder werd aangenomen. De oorspronkelijke formele definitie van NR in het plain model, voorgesteld door Cremers *et al.*, blijkt inderdaad onhaalbaar te zijn, en hetzelfde geldt voor de natuurlijke uitbreiding van NR naar het random oracle model. De onhaalbaarheid wordt gepresenteerd in de vorm van een eenvoudige concrete aanval die van toepassing is op alle "natuurlijke" algoritmes (hoewel er een kleine technische opening blijft voor de "onnatuurlijke" algoritmes). In het bijzonder omvat het alle handtekeningenalgoritmes die gebruikmaken van de BUFF transformatie, en daarmee wordt de eerder geclaimde veiligheid van BUFF ongeldig verklaard.

De bovengenoemde aanval vormt echter geen echte bedreiging voor de beoogde toepassingen van NR. In plaats daarvan laat dit zien dat de oorspronkelijke formele definitie van NR ontoereikend is. Om deze negatieve situatie te verhelpen, gaan we terug naar de tekentafel: we stellen meerdere nieuwe formele definities voor en onderzoeken de haalbaarheid van deze definities. Uiteindelijk verkrijgen we zowel positieve als negatieve resultaten. Enerzijds tonen we aan dat de BUFF transformatie inderdaad voldoet aan enkele zinvolle definities van NR, terwijl anderzijds is de haalbaarheid van NR nog steeds sterk afhankelijk van de subtiele details van de formele definitie.

In Hoofdstuk 5 bestuderen we een *KEM samensteller*. Dat is een generieke compiler die meerdere key-encapsulation mechanisms (KEMs) omzet in een gecombineerde KEM, die veilig is als minstens één van de onderliggende KEM's veilig is. Met een dergelijke samensteller zou men een gevestigde pre-quantum KEM, bijvoorbeeld op basis van RSA of Diffie-Hellman, kunnen samenstellen met een nieuw post-quantum algoritme, waardoor partijen soepeler kunnen overstappen op post-quantum cryptografische algoritmes met minder risico's.

Wat we overwegen, is een bijzonder efficiënte constructie die is voorgesteld door Giacon, Heuer en Poettering die gebaseerd is op de veiligheid van een split-key pseudorandom function (skPRF). Omdat de belangrijkste toepassing hiervan in de context van post-quantum cryptografie is, bewijzen we dat deze skPRF veilig blijft tegen quantumaanvallen en dat daardoor ook de bijbehorende KEM samensteller veilig is tegen quantumaanvallen.