Samenvatting

Deze dissertatie draagt bij aan de theorie van multi-prover commitment schemes, in het bijzonder relativistische commitment schemes. Een *commitment scheme* is een cruciale bouwsteen voor cryptografische protocollen welke meerdere partijen die elkaar niet vertrouwen in staat stellen om op een veilige manier samen te werken. Meer specifiek beschouwen wij multi-prover commitment schemes waarvan de veiligheid gebaseerd is op veronderstelde beperkingen op de communicatie tussen de provers, en niet op aannamen over de computationele complexiteit van wiskundige problemen.

Een commitment scheme is een middel om het volgende probleem op te lossen: Alice heeft een bericht geschreven die zij eerst geheim wil houden, maar die zij mogelijk later aan Bob wil onthullen. Echter, als zij het bericht eenvoudigweg op een latere tijd aan Bob zou sturen, weet Bob niet zeker of het bericht dat hij ontving gelijk is aan het bericht dat zij eerder heeft geschreven. Een commitment scheme zorgt ervoor dat het bericht geheim blijft totdat Alice het wil onthullen, maar ook dat Alice geen ander bericht aan Bob kan onthullen.

Een commitment scheme is formeel gedefinieerd als een tweetal interactieve protocollen tussen (meestal) twee partijen, genoemd de *prover* en de *verifier*. Het eerste protocol, genoemd de *commit* fase, neemt een bericht van de prover als input en geen input van de verifier. Het tweede protocol, genoemd de *opening* fase, geeft dan een bericht uit aan de verifier, of $\perp$ om aan te geven dat de prover er niet in geslaagd is om het commitment te openen. Als de output een bericht m is, zegt men dat de prover het commitment naar m geopend had. Vaak stuurt de prover in de opening fase alleen zogenoemde *opening information* aan de verifier die dan lokaal de output berekent.

Om veilig te zijn moet een commitment scheme de volgende eigenschappen hebben: het moet *compleet* zijn, d.w.z. dat de input van de commit fase gelijk is aan de output van de opening fase als beide partijen de protocollen volgen. Het moet *verbergend* zijn, d.w.z. dat de verifier de input van de prover niet voor de opening fase kan uitvinden, ook als de verifier oneerlijk is en van de protocollen afwijkt. Het moet *bindend* zijn, d.w.z. dat de prover na de commit fase maar naar één bericht kan openen, ook als de prover oneerlijk is en van de protocollen afwijkt. De verzameling van mogelijke inputs van een commitment

scheme wordt zijn *domein* genoemd. Als het domein de verzameling $\{0, 1\}$ is, spreken we van een *bit*-commitment scheme.

Een standaard commitment scheme kan alleen veilig zijn als tenminste één van de partijen beperkte rekenkracht heeft. Dit is echter alleen waar als er maar één prover is. Ben-Or, Goldwasser, Kilian en Wigderson bewezen in 1988 dat deze beperking omzeild kan worden door een variant van commitment schemes waar de prover opgesplitst wordt in twee (of meer) aparte entiteiten die per aanname gedurende de uitvoering van het commitment scheme niet kunnen communiceren. Gerelateerd aan dit idee is het idee van *relativistische commitment schemes*, dat in 1999 door Kent werd voorgesteld: door de provers ver van elkaar te plaatsen is het mogelijk om tijdelijk aan de aanname te voldoen dat de provers niet kunnen communiceren.

De eerste hoofdbijdrage van deze dissertatie zijn nieuwe definities voor het bindend-zijn van een multi-prover commitment scheme. Deze nieuwe definities hebben meerdere voordelen boven de tot nu gebruikte *sum-binding* definitie: ze zijn niet beperkt tot *bit*-commitment schemes, maar van toepassing voor commitment schemes met arbitraire eindige domeinen. Voor bit-commitment schemes zijn sommige van onze definities *strikt sterker* dan de sum-binding definitie. Verder blijven onze definities dichter bij de intuïtie en zijn makkelijker te gebruiken. Wij stellen deze definities voor en bestuderen de relaties tussen hen.

Om onze definities te testen gebruiken wij het $\mathcal{CHSH}^q$ bit-commitment scheme – geïntroduceerd door Crépeau, Salvail, Simard en Tapp – die op een natuurlijke manier uitgebreid kan worden naar een commitment scheme met domein $\mathbb{F}_q$ (waar q een macht van een priemgetal is). Wij analyseren het voor het eerst als een commitment scheme voor dit grotere domein en bewijzen dat verschillende varianten van het commitment scheme aan verschillende definities voldoen.

Onze nieuwe definities stellen ons in staat om een vrij algemene *compositie-stelling* voor two-prover commitment schemes te bewijzen, de tweede hoofdbijdrage van deze dissertatie. Wij voegen twee commitment schemes samen door de provers aan de *opening information* van het eerste scheme te laten committen met het tweede scheme, en dan dit tweede commitment te openen. Dit onthult de opening information en het eerste commitment wordt dus geopend. Wij bewijzen dat het samengestelde scheme bindend is als de twee originele schemes bindend zijn en aan enkele lichte verdere eisen voldoen. (De succeskans voor oneerlijke provers in het samengestelde commitment scheme is de som van hun succeskansen in de twee originele schemes.)

Het doel van deze compositie is het openen van het commitment te vertragen. Dit is belangrijk in de context van relativistische commitment schemes, waar de aanname dat de provers niet kunnen communiceren alleen tijdelijk geldig is.

Concreet maakt onze compositie-stelling een betere analyse mogelijk van het relativistische commitment scheme dat door Lunghi, Kaniewski, Brussiè-

res, Houlman, Tomamichel en Wehner in 2015 werd voorgesteld. Hun originele analyse bewees een bovengrens aan de succeskans van oneerlijke provers die dubbel exponentieel was in het aantal communicatie-ronden, dat bepaalt hoe lang het commitment scheme bindend zal blijven. Het scheme kan beschouwd worden als een iteratieve compositie van $\mathcal{CHSH}^q$ met zichzelf, en dus kunnen wij het met behulp van onze compositie-stelling analyseren. Op deze manier bereiken wij een enorme verbetering van het resultaat van Lunghi *et al.*: wij bewijzen dat de succeskans van oneerlijke provers lineair is in het aantal communicatie-ronden, en niet dubbel exponentieel. We bewijzen ook dat ons resultaat optimaal is, op een klein constante factor na.

Meer concreet: Lunghi *et al.* hebben hun commitment scheme met provers in Bern en Genève (afstand: 192.2 km) geïmplementeerd. Volgens hun analyse bleef het scheme bindend (met een redelijk lage succeskans voor oneerlijke provers) voor 2 ms. Onze analyse bewijst dat een duur van 10^{56} jaar met dezelfde grens aan de succeskans mogelijk is – of, meer praktisch, totdat de geheugens van de apparaten vol zijn.

De derde hoofdbijdrage is een bewijs dat er geen two-prover commitment schemes bestaan die veilig zijn tegen algemene *non-signaling provers*. Zoals bewezen door Crépeau, Salvail, Simard en Tapp moet de niet-communicatie premisse verder worden uitgewerkt. Sommige commitment schemes zijn veilig tegen klassieke oneerlijke provers, maar onveilig tegen provers die een verstrengelde kwantumtoestand delen. Wil men nog verder gaan en de veiligheid van een commitment scheme echt alleen bouwen op de aanname dat de provers niet kunnen communiceren, moet men algemene non-signaling provers beschouwen. Dit betekent dat het gedrag van de provers op welke manier dan ook gecorreleerd kan zijn, zolang het geen communicatie tussen hen impliceert. $\mathcal{CHSH}^q$ is veilig tegen provers met kwantumverstrengeling, maar niet tegen algemene non-signaling provers. Dit werpt de vraag op of een ander commitment scheme wel veilig tegen zulke provers is.

Wij bewijzen dat dit voor *two-prover* commitment schemes niet het geval is: een commitment scheme dat compleet en verbergend is kan niet bindend zijn voor algemene non-signaling provers. Anderzijds hebben wij ook een positief resultaat: wij bewijzen dat een eenvoudige uitbreiding van $\mathcal{CHSH}^q$ naar een *three-prover* commitment scheme compleet, verbergend voor een arbitraire oneerlijke verifier, en bindend voor algemene non-signaling provers is.