Compressed Σ-protocol theory

Attema, T.

SAMENVATTING

Samenvatting

Het vakgebied van de *(probabilistische) bewijssystemen* heeft zich ontwikkeld tot een bloeiend deelgebied binnen de cryptologie en informatica. In analogie met wiskundige bewijzen, is het doel van een bewijssysteem dat een bewijzer een verificateur kan overtuigen van de juistheid van een bewering. Probabilistische bewijzen laten daarentegen toe dat de verificateur fouten maakt, dat wil zeggen onjuiste beweringen accepteert (*degelijkheidsfout*) of correcte beweringen verwerpt (*volledigheidsfout*). In veel gevallen kan de foutkans door herhaling verwaarloosbaar klein gemaakt worden zonder veel aan efficiëntie in te leveren. Dit is voor de meeste praktische toepassingen voldoende. Verder kunnen probabilistische bewijzen meerdere interactierondes tussen de bewijzer en de verificateur hebben. In dit geval worden probabilistische bewijzen ook wel *interactieve bewijzen* genoemd. Deze veralgemening, geïntroduceerd door Babai, Goldwasser, Micali en Rackoff [Bab85; GMR85], zorgde voor een revolutie in de bewijstheorie. Door absolute zekerheid in te ruilen voor hoge waarschijnlijkheid en interactie toe te staan, is het bijvoorbeeld mogelijk beweringen te bewijzen zonder meer te onthullen dan hun juistheid. Deze eigenschap wordt *nul-kennis* (zero-knowledge) genoemd. Tegenwoordig worden nul-kennis bewijzen op grote schaal ingezet; ze zijn bijvoorbeeld essentieel in de publieke sleutel infrastructuren die digitale identiteiten en beveiligde communicatiekanalen op het internet beheren.

In het bijzonder biedt de theorie van de Σ-protocollen [Cra96] nu een sterke basis voor het modulair ontwerpen van nul-kennis bewijssystemen in een breed scala aan toepassingsdomeinen. Een Σ-protocol is een interactief bewijs met drie rondes; de bewijzer stuurt eerst een bericht naar de verificateur, die antwoordt met een *challenge* die uniform willekeurig is gekozen uit een eindige verzameling, en na ontvangst van een antwoord van de bewijzer beslist de verificateur om de bewering van de bewijzer te accepteren of af te wijzen. De theorie van de Σ-protocollen onderscheidt zich door haar *modulariteit*; elementaire Σ-protocollen zijn elegant en gemakkelijk te analyseren, en complexe toepassingsscenario's worden afgehandeld door deze basisbouwstenen op de juiste manier te combineren. Op deze manier kan bijvoorbeeld de *vervulbaarheid* van een aritmetisch circuit $C\colon \mathbb{Z}_q^n \to \mathbb{Z}_q$ bewezen worden [CD98], waar $\mathbb{Z}_q$ de ring van gehele getallen modulo q is. Preciezer gezegd, met behulp van de juiste Σ-protocollen kan een bewijzer laten zien dat C een input $\mathbf{x} \in \mathbb{Z}_q^n$ heeft waarvoor geldt dat $C(\mathbf{x}) = 0$. Sterker nog, Σ-protocollen bieden een krachtigere functionaliteit; ze stellen bewijzers in staat om niet alleen te bewijzen dat een circuit vervulbaar is, maar ook dat ze een bijbehorende oplossing $\mathbf{x} \in \mathbb{Z}_q^n$ kennen. Deze eigenschap wordt *kennisdegelijkheid* (knowledge soundness) genoemd, en interactieve bewijzen met deze eigenschap worden ook wel *bewijzen van kennis* genoemd. Het circuit-vervulbaarheidsprobleem is NP-compleet, wat betekent dat elk probleem waarvoor oplossingen efficiënt verifieerbaar zijn, kan

worden geschreven als een circuit-vervulbaarheidsprobleem. Daarom kan door middel van een Σ-protocol elke efficiënt verifieerbare bewering in nul-kennis bewezen worden. Vanwege de modulariteit van de Σ-protocoltheorie zijn er voor veel toepassingsscenario's echter directere en efficiëntere oplossingen die de vaak omslachtige reductie tot een circuit-vervulbaarheidsprobleem vermijden.

Probabilistische bewijzen hebben verschillende prestatiemetrieken, die bijvoorbeeld de (rekenkundige) complexiteit aangeven van het genereren of verifiëren van een bewijs. De communicatiekosten vormen een andere belangrijke metriek; het aantal bits dat wordt gecommuniceerd tussen de bewijzer en de verificateur. Helaas groeien voor veel toepassingsscenario's de communicatiekosten van standaard Σ-protocollen *lineair* met de omvang van de probleeminstantie. Zo is de communicatiecomplexiteit van een Σ-protocol voor het circuit-vervulbaarheidsprobleem lineair in de grootte van het aritmetische circuit. Meer recentelijk is een vouwtechniek geïntroduceerd om de communicatiecomplexiteit te verminderen van lineair naar logaritmisch in de grootte van de probleeminstantie [BCC+16; BBB+18]. De resulterende protocollen worden Bulletproofs genoemd. Bulletproofs werden geïntroduceerd als een vervanging voor Σ-protocollen in verschillende toepassingen, zoals nul-kennis bewijzen voor circuit-vervulbaarheid.

In dit proefschrift verzoenen we de vouwtechniek van Bulletproofs met de gevestigde Σ-protocoltheorie. We laten zien dat de vouwtechniek kan worden gezien als een significante *versterking*, in plaats van een vervanging, van Σ-protocollen. Ons uitgangspunt is een elementair Σ-protocol voor het bewijzen van kennis van een *origineel* van een publiek element $P \in \mathbb{H}$ in het codomein van een groepshomomorfisme $\Psi\colon \mathbb{G}^n \to \mathbb{H}$. Nauwkeuriger gezegd stelt dit Σ-protocol een bewijzer in staat om kennis van een geheime inputvector $\mathbf{x} \in \mathbb{G}^n$ te bewijzen, waarvoor geldt dat $\Psi(\mathbf{x}) = P$ voor een publieke $P \in \mathbb{H}$. De communicatiekosten van dit Σ-protocol groeien lineair in $n \in \mathbb{N}$. Vervolgens laten we zien dat de communicatiecomplexiteit, door een aanpassing van de vouwtechniek van Bulletproofs, kan worden gereduceerd tot logaritmisch in n (of polylogaritmisch, afhankelijk van de concrete instantiëring). Vergelijkbaar met Bulletproofs gaat deze verbetering ten koste van een logaritmisch, in plaats van een constant, aantal rondes. Omdat dit compressiemechanisme hier wordt beschouwd als een uitbreiding van een elementair Σ-protocol, kunnen veel technieken bekend uit de Σ-protocoltheorie direct worden overgenomen door deze nieuwe *theorie van de gecomprimeerde Σ-protocollen*.

Verder breiden we de theorie van de gecomprimeerde Σ-protocollen uit met twee aanvullende functionaliteiten. Ten eerste, door middel van een techniek gebaseerd op aritmetische *secret-sharing*, laten we zien hoe de juistheid van m vermenigvuldigingsdrietallen (multiplication triples) $(\alpha_i, \beta_i, \gamma_i = \alpha_i \cdot \beta_i) \in \mathbb{Z}_q^3$ kan worden bewezen $(1 \leq i \leq m)$. Nauwkeuriger gezegd wordt het bewijzen van de juistheid van vermenigvuldigingsdrietallen gereduceerd tot het bewijzen van kennis van een origineel van een homomorfisme. In andere woorden, de niet-lineaire vermenigvuldigingsdrietal-relatie wordt gelineariseerd. Deze aanpak is bekend uit de Σ-protocoltheorie [CDM00; CDP12] en is geïnspireerd door secure multiparty computation [CDN15]. Er zijn echter enkele aanpassingen nodig om deze aanpak geschikt te maken voor compressie. Door een gepaste en efficiënte reductie laten we zien dat deze functionaliteitsverbetering voldoende is om de vervulbaarheid van aritmetische circuits in (poly)logaritmische communicatie te bewij-

zen. Als tweede functionaliteitsverbetering construeren we een nieuw k-uit-n bewijs van partiële kennis, waarmee kennis van k-uit-n originelen van een homomorfisme bewezen kan worden zonder te onthullen welke originelen de bewijzer kent. Bewijzen van partiële kennis, met name 1-uit-n, hebben de afgelopen decennia talloze toepassingen gevonden, bijvoorbeeld in elektronisch stemmen, digitale (ring)handtekeningen en vertrouwelijke transactiesystemen. Onze constructie laat zien hoe de communicatiecomplexiteit kan worden teruggebracht van lineair naar (poly)logaritmisch in k en n. We vermijden het gebruik van generieke reducties naar circuit-vervulbaarheid en identificeren praktische toepassingsscenario's waarbij onze aanpak asymptotische en concrete prestatieverbeteringen oplevert.

De theorie van de gecomprimeerde Σ-protocollen wordt gepresenteerd in een eenvoudige en abstracte taal, waardoor instantiëringen in diverse cryptografische platforms mogelijk zijn. In het bijzonder laten we zien hoe gecomprimeerde Σ-protocollen geïnstantieerd kunnen worden op basis van de discrete logaritme aanname, resulterend in een logaritmische communicatiecomplexiteit. Vervolgens laten we zien hoe deze instantiëring kan worden uitgebreid naar platforms gebaseerd op bilineaire *pairings*. Op basis van de *kennis van de exponent* (knowledge of exponent) aanname kan de communicatiecomplexiteit verder worden teruggebracht naar een constante hoeveelheid. Ten slotte presenteren we strong-RSA en roostergebaseerde instantiëringen, waarbij het aannemelijk is dat de laatste aanname post-quantum veiligheid biedt. Strong-RSA en op roosters gebaseerde instantiëringen zijn onderhevig aan een zogenaamde *degelijkheidsmarge* (soundness slack). Omgaan met een degelijkheidsmarge vereist grotere protocolparameters en zorgt ervoor dat de resulterende communicatiecomplexiteit polylogaritmisch is in plaats van logaritmisch of constant.

Verder identificeren en dichten we drie hiaten in de algemene theorie van interactieve bewijzen met meerdere rondes. Deze resultaten zijn in het bijzonder relevant voor Bulletproofs en gecomprimeerde Σ-protocollen. Het is over het algemeen namelijk niet triviaal om aan te tonen dat een interactief bewijs *kennisdegelijk*, en dus een bewijs van kennis, is en om een goede bovengrens te vinden voor de *kennisfout*, die de kans op succes van een oneerlijke bewijzer aangeeft. Daarom werd in de context van Σ-protocollen de meer handteerbare notie *speciale-degelijkheid* (special-soundness) geïntroduceerd [Cra96]. Het is bekend dat speciale-degelijkheid, of nauwkeuriger gezegd 2-uit-N speciale-degelijkheid, kennisdegelijkheid met kennisfout $1/N$ impliceert, waarbij N de grootte van de challenge-verzameling van de verificateur is. Algemener impliceert k-uit-N speciale-degelijkheid kennisdegelijkheid met kennisfout $(k-1)/N$. Bulletproofs en gecomprimeerde Σ-protocollen hebben natuurlijke generalisaties van speciale-degelijkheid, voor interactieve bewijzen met meerdere rondes, relevant gemaakt.

Het eerste open probleem dat we aanpakken, is het ontbreken van een kennisdegelijkheidsanalyse voor speciaal-degelijke interactieve bewijzen met meerdere rondes. Als de gevonden bovengrens van de kennisfout niet minimaal is, moeten er conservatieve protocolparameters gebruikt worden. Dit maakt concrete instantiëringen onnodig inefficiënt. Wij bieden de eerste analyse voor de brede klasse van speciaal-degelijke interactieve bewijzen met meerdere rondes die resulteert in een minimale bovengrens voor de kennisfout.

Het tweede open probleem onderzoekt het effect van parallelle herhaling op de

kennisfout. In veel gevallen is de kennisfout κ niet klein genoeg en moet deze dus worden verkleind. Dit kan worden gedaan door het interactieve bewijs parallel te herhalen. Het effect van parallelle herhaling op 2-uit-N speciaal-degelijke Σ-protocollen is bekend, maar de situatie wordt aanzienlijk ingewikkelder als we kijken naar k-uit-N speciale-degelijkheid voor $k > 2$. De situatie wordt al helemaal complex wanneer we de generalisaties van speciale-degelijkheid voor interactieve bewijzen met meerdere rondes beschouwen. Het is namelijk gemakkelijk in te zien dat de t-voudige parallelle herhaling van een 2-uit-N speciaal-degelijk interactief bewijs 2-uit-N^t speciaal-degelijk is. Deze parallelle herhaling heeft dus kennisfout $1/N^t$. Een soortgelijk resultaat geldt niet voor de generalisaties van speciale-degelijkheid. We lossen dit probleem op door te bewijzen dat, voor alle interactieve bewijzen die deze generaliseerde speciale-degelijkheid eigenschap bezitten, t-voudige parallelle herhaling de kennisfout optimaal reduceert van κ tot κ^t.

Ten derde analyseren we de Fiat-Shamir transformatie van speciaal-degelijke interactieve bewijzen met meerdere rondes. De Fiat-Shamir transformatie is een veelgebruikte heuristiek die een public-coin[1] interactief bewijs niet-interactief maakt door de berichten van de verificateur te vervangen door bepaalde hashfunctie-evaluaties. Helaas gaat de Fiat-Shamir transformatie gepaard met een gereduceerde veiligheid van het protocol. Dit verlies kan zelfs *exponentieel* in het aantal rondes van het interactieve bewijs zijn, wat een negatief effect heeft op het kiezen van concrete protocolparameters. Als men wil vertrouwen op bewezen veiligheid, moet men grote parameters kiezen voor het interactieve bewijs om het exponentiële verlies te compenseren. Dit beïnvloedt de efficiëntie op een negatieve manier. Als alternatief kan de bewezen veiligheid opgegeven worden en simpelweg aangenomen worden dat het verlies in veiligheid veel milder is dan wat de algemene (exponentiële) grens suggereert. Het is inderdaad zo dat voor veel interactieve bewijzen de bekende aanvallen geen exponentieel verlies vertonen. Aannemen dat het verlies milder is, is een gangbare praktijk geworden. In dit proefschrift laten we zien dat voor interactieve bewijzen met speciale-degelijkheid het veiligheidsverlies *onafhankelijk* is van het aantal rondes. Men kan nu vertrouwen op bewezen veiligheid zonder al te conservatieve en dus inefficiënte protocolparameters te kiezen.

Ten slotte construeren we, als toepassing van gecomprimeerde Σ-protocollen, een nieuw k-uit-N *Threshold Signature Scheme* (TSS). De TSS is compact omdat een threshold signature een grootte heeft die sublineair is in k en n. Verder vereist onze TSS, in tegenstelling tot andere compacte TSS'en, geen vertrouwde partij om de publieke protocolparameters te genereren. Een TSS met deze eigenschap wordt transparant genoemd. Door de modulaire aard van de theorie van de gecomprimeerde Σ-protocollen verwachten wij dat veel meer toepassingsscenario's op een intuïtieve en efficiënte manier benaderd kunnen worden.

[1] Een interactief bewijs wordt *public-coin* genoemd als de verificateur al zijn willekeur (randomness) publiek maakt gedurende een protocol executie.