

CISPA-Stanford Center



FOR CYBERSECURITY

Projekt Stanford_2018

- Schlussbericht -

Zuwendungsempfänger:	CISPA - Helmholtz-Zentrum für Informationssicherheit gGmbH
Förderkennzeichen:	16KIS0927
Projektleitung:	Prof. Dr. Dr. h. c. Michael Backes / Dr. Theo Jäger
Laufzeit des Vorhabens:	01.09.2018-30.09.2024

Inhalt

1	Kurze Darstellung.....	3
2	Eingehende Darstellung.....	4
2.1	Inhalt und Ergebnisse.....	4
2.2	Anwendungsmöglichkeiten.....	6
2.3	Kollaborationen.....	8
3	Publikationsliste	9

1 Kurze Darstellung

Die weiter zunehmende Digitalisierung und Vernetzung unserer Welt bringt enorme Herausforderungen speziell in der Informationssicherheit mit sich, mit denen sowohl Forschung als auch Industrie konfrontiert sind. Vor diesem Hintergrund wurde im Jahr 2017 das CISPA-Stanford Center for Cybersecurity (CSC) als Kooperation zwischen dem CISPA Helmholtz-Zentrum für Informationssicherheit in Saarbrücken und der Stanford University in Kalifornien/USA etabliert. Kernziel des CSC ist es, mit einem innovativen Qualifizierungskonzept exzellenten wissenschaftlichen Nachwuchs zu hochausgebildeten Fach- und Führungskräften für Forschung und Industrie im Bereich der Informationssicherheit zu entwickeln. Dadurch können das CISPA und das gemeinsame CSC-Programm mit der Stanford University bedeutsam dazu beitragen, die Wettbewerbsfähigkeit von Europa und speziell des Standorts Deutschland im Zukunftsfeld der Cybersicherheit zu unterstützen.

Das Qualifizierungsprogramm des CSC ist in drei unterschiedliche Phasen strukturiert:

- **Phase 1:** Je nach vorheriger Qualifikation üben die teilnehmenden Wissenschaftler:innen ein bis zwei Jahre lang eine forschende Tätigkeit als Postdoktorand:innen am CISPA aus. Hierdurch wird sichergestellt, dass sie die erforderliche Qualifizierung und wissenschaftliche Selbständigkeit für die darauffolgende Phase erlangen. Zudem werden sie eng in das Forschungsumfeld des CISPA integriert und an den Forschungs- und Industriestandort Deutschland herangeführt bzw. daran gebunden.
- **Phase 2:** Die teilnehmenden Wissenschaftler:innen verbringen anschließend einen zweijährigen Aufenthalt an der renommierten Stanford University mit dem attraktiven Status als Visiting Assistant Professor. Der Aufenthalt in Stanford ermöglicht es ihnen, an einem der weltweit führenden Standorte in einem exzellenten Forschungsumfeld das amerikanische Wissenschaftssystem kennenzulernen und ihr akademisches Profil weiter zu schärfen. Diese Erfahrung ermöglicht es den Teilnehmenden, sich thematisch zu profilieren und an neuartigen Fragestellungen zu forschen. Sie betreuen zudem Promovierende und Studierende der Stanford University, die sich am CSC beteiligen. Die Nachwuchswissenschaftler:innen wurden während ihres Aufenthalts an der Stanford University eng in die dortigen Gruppen eingebunden und in die Lehre integriert. Die in den USA entstandenen Netzwerke wurden nach der Rückkehr in das deutsche Wissenschaftssystem weiter gepflegt. Dies spiegelt sich in zahlreichen gemeinsamen Arbeiten und Publikationen wider, die oft auch erst nach Abschluss des USA-Aufenthaltes entstehen.
- **Phase 3:** Nach ihrer Rückkehr ins deutsche Forschungsumfeld am CISPA fließen die in Stanford gewonnenen Erkenntnisse in die weitere Forschungs- und Lehrtätigkeit der Wissenschaftler:innen ein. Sie sammeln nun maximal drei Jahre als Nachwuchsgruppenleiter:innen weitere Erfahrungen und betreuen vor Ort weiterhin Promovierende und Studierende des CISPA, die sich am CSC beteiligen.

Die während dieser Programmphasen erlangte wissenschaftliche Exzellenz der Teilnehmenden spiegelt sich in zahlreichen hochrangigen Forschungspublikationen und auch in besonderen Auszeichnungen auf renommierten Konferenzen im Bereich der IT-Sicherheit wider, die sie für ihre Arbeiten erhielten. Des Weiteren etablieren die Teilnehmenden während ihrer Tätigkeit im CSC-Programm ein breites Spektrum an Kooperationen in Forschung und Industrie,

die ihnen in den jeweiligen wissenschaftlichen Projekten zugutekommen. Dank der im CSC erlangten hohen Qualifikation können sich die Teilnehmenden spätestens gegen Ende der Phase 3 erfolgreich auf Leitungspositionen in Wissenschaft oder Industrie bewerben, sowohl in Deutschland als auch im internationalen Kontext. Durch die fortbestehende Vernetzung auch über die Programmphase hinaus entwickeln sich längerfristige Kontakte und dadurch Möglichkeiten für neue Kooperationen mit externen (insbesondere Forschungs-)Einrichtungen, an denen die Teilnehmenden des CSC ihre Anschlusspositionen erlangt haben.

Organisatorisch wird das Zentrum in Saarbrücken und in Stanford durch den jeweiligen Direktor geleitet. Am CISPA liegt die Leitung bei Herrn Prof. Michael Backes und an der Stanford University bei Prof. John Mitchell. Zudem unterstützen in Stanford Prof. Dan Boneh und Prof. David Mazières bei der Betreuung der Teilnehmenden. Die Zusammenarbeit zwischen den beiden renommierten Institutionen wurde durch den stetigen Austausch von exzellenten Nachwuchskräften intensiviert und erfuhr zahlreiche neue Facetten. Die Geschäftsstelle des CSC wurde in die Aufgaben des Wissenschaftssupports am CISPA integriert, wodurch der Aufwand für die Koordination des Programms aus der Grundfinanzierung des Zentrums getragen werden kann. Die Ansprechpartner:innen der Geschäftsstelle stehen den teilnehmenden Wissenschaftler:innen jederzeit beratend zur Verfügung.

Seit der Einrichtung des CSC hat sich das gemeinsame Programm mit der Stanford University als fruchtbares Instrument der wissenschaftlichen Qualifizierung und Karriereförderung für die teilnehmenden Forschenden herausgestellt. Dies widerspiegelt sich auch in einer Evaluation des Programms, die im Jahr 2021 durch den wissenschaftlichen Beirat des CSC durchgeführt wurde. Auf Basis eines Berichts und von Vorträgen durch die Programmbeteiligten wurde ein Gutachten vorgelegt, das ein positives Urteil über die bisherige Projektlaufzeit und die nachdrückliche Empfehlung zur Fortsetzung des Programms durch den wissenschaftlichen Beirat enthielt.

2 Eingehende Darstellung

2.1 Inhalt und Ergebnisse

Die erste Kohorte des CSC startete im Jahr 2017 mit vier Teilnehmenden, die sich dank der während des Programms gesammelten Erfahrungen und erlangten Qualifikationen rasch und erfolgreich auf Führungspositionen in der Wissenschaft bewerben konnten. Die Ausschreibung für die im Rahmen dieses Projekts geförderte zweite Kohorte wurde Ende 2017 veröffentlicht und lief bis Februar 2018. Der vorliegende Bericht geht auf diese zweite Kohorte des CISPA-Stanford Centers ein, die mit zwei Teilnehmenden gestartet ist.

Dr. Hojoon Lee, der 2018 am renommierten Korea Advanced Institute of Science and Technology promoviert wurde, trat am 01.09.2018 in das Programm ein, erhielt aber bereits frühzeitig während Phase 1 ein attraktives Stellenangebot der Sungkyunkwan University in Südkorea über eine Position als Associate Professor am Department of Computer Science and Engineering. Dieses nahm er zum 01.08.2019 an und schied hierdurch aus dem CSC-Programm aus, bevor er einen Forschungsaufenthalt an der Stanford University antreten konnte.

Dr. Kamil Kluczniak, der 2016 an der Polnischen Akademie der Wissenschaften promoviert wurde, trat am 01.09.2018 als Postdoktorand in das Programm in Phase 1 ein und nahm ein

Jahr später am 01.09.2019 die Phase 2 auf. Seine zwei Jahre als Visiting Assistant Professor an der Stanford University waren auch von der Corona-Situation geprägt, denn in Stanford wurde bereits früh Homeoffice angeordnet und der Zutritt zum Campus und insbesondere den Bürogebäuden war nur bestimmten Personengruppen vorbehalten. Dr. Kluczniak beteiligte sich daher nach Möglichkeit an den Online-Aktivitäten des CISPA und der Stanford University. Im Vordergrund stand dabei der wissenschaftliche Austausch. Er kehrte am 01.10.2021 zur Phase 3 als Nachwuchsgruppenleiter ans CISPA nach Saarbrücken zurück und baute anschließend seine Forschungsgruppe auf, wobei dies aufgrund der Corona-Situation weiterhin unter erschwerten Bedingungen geschah. Ein von ihm rekrutierter Doktorand trat am 01.05.2022 eine Promotionsstelle unter seiner Betreuung an. Eine weitere Promotionsstelle von Dr. Kluczniak blieb unbesetzt, weil sich der Visumsprozess für einen geeigneten Kandidaten mit chinesischer Staatsbürgerschaft zu lange hinzog.

Dr. Kluczniak befasste sich während seiner Beteiligung am CSC hauptsächlich mit praktischen Aspekten der sicheren Berechnung, wobei der Schwerpunkt auf Techniken der vollständig homomorphen Verschlüsselung (fully homomorphic encryption; FHE) lag. FHE ist eine Technik, die es ermöglicht, Daten zu verschlüsseln und den Chiffretext an einen nicht vertrauenswürdigen Server zu senden, der mit den verschlüsselten Daten eine beliebige Berechnung durchführen und das Ergebnis der Berechnung zurücksenden kann. Mit einem speziellen geheimen Schlüssel kann das Ergebnis der Berechnung des Servers dann effizient wiederhergestellt werden. Dr. Kluczniak engagierte sich außerordentlich im Hinblick auf den Aufbau dieses in Deutschland stark vernachlässigten Forschungsgebiets innerhalb der Kryptografie und den damit verbundenen praxisorientierten Anwendungsmöglichkeiten. Er trug maßgeblich und eigenständig dazu bei, dass in Deutschland erstmalig eine vertiefte Expertise in diesem Forschungsgebiet aufgebaut wurde.

Während der Tätigkeit im CSC-Programm haben Dr. Kluczniak und seine Gruppe neue FHE-Techniken entwickelt, die den derzeitigen Stand der Technik in der Praxis deutlich übertreffen. Insbesondere haben sie eine Methode namens „Functional Bootstrapping“ generiert, die bei praktischen Berechnungen mit verschlüsselten Daten eine über 1.000-fache Beschleunigung gegenüber früheren Methoden erzeugt. Die Gruppe hat das erste praxistaugliche FHE-Schema eingeführt und implementiert, das auf der NTRU-Annahme basiert und zu einer nicht-trivialen Beschleunigung führt. Insbesondere wurden neue Bereinigungsverfahren entwickelt, um die Sicherheitseigenschaften von einfacher FHE durch den Schutz von Schaltkreisen zu ergänzen, was für Anwendungen von FHE bei sicheren Mehrparteienberechnungen von entscheidender Bedeutung ist. Darüber hinaus hat Dr. Kluczniak zusammen mit seinem Doktoranden den aktuellen Stand der Technik von Schwellenwert-FHE analysiert. In Zusammenarbeit mit der Ruhr-Universität Bochum wurde einer der ersten Compiler entwickelt, der in der Lage ist, in C++ geschriebenen Code zu einer spezifischen Schaltung zu kompilieren, die über verschlüsselte Daten verarbeitet werden kann. Letztendlich wurden alle praktischen Ergebnisse implementiert und zur Demonstration in Form einer Open-Source-Bibliothek zur Verfügung gestellt.

FHE ist mit zahlreichen Anwendungsmöglichkeiten in den Bereichen Kryptographie sowie datenschutzfreundliches Cloud Computing und kollaboratives Computing verbunden. FHE ist in den letzten Jahren deutlich praxistauglicher geworden, was renommierte Unternehmen wie IBM, Microsoft oder Google und auch Start-ups dazu veranlasst hat, umfangreiche Mittel und Aufmerksamkeit in die Entwicklung neuer und effizienter FHE-Techniken zu investieren. Die wichtigsten Forschungs- und Startup-Zentren, die sich mit FHE beschäftigen, befinden sich jedoch derzeit in den USA, Frankreich und Korea. In Deutschland gibt es hingegen einen Mangel an Einrichtungen und Gruppen in der Forschung oder Industrie, die sich mit FHE beschäftigen.

Daher bestand das Hauptziel der Tätigkeit von Dr. Kluczniak darin, die erste Forschungsgruppe in Deutschland aufzubauen, die sich in erster Linie auf die Entwicklung neuer praxisrelevanter FHE-Methoden konzentriert. Die dabei erzielten Methoden sollen mit internationalen Technologien konkurrieren können und unterstützten damit den Erwerb von Fachwissen für eine mögliche Vermarktung und Anwendung der Technologie durch die Industrie und die Politik innerhalb Deutschlands.

Mit dem 31.12.2023 schied Dr. Kluczniak aus dem Programm aus, da er nach seiner Forschungstätigkeit am CISPA in die einschlägige Industrie gewechselt ist und im Raum München als Senior-Berater bei einem der führenden Cybersecurity-Unternehmen Deutschlands (secunet Security Networks AG) tätig wurde. Auch nach seinem Wechsel in die Industrie erhält weiterhin Anfragen auf Forschungs Kooperationen im Themenbereich der FHE von deutschen Universitäten und Unternehmen, auf die er allerdings aufgrund seiner neuen Tätigkeit außerhalb der Forschung nicht vollständig eingehen kann.

Der von Dr. Kluczniak eingestellte Doktorand arbeitet aktuell weiterhin am CISPA an seiner Doktorarbeit unter der Betreuung von Prof. Antoine Joux, wobei der Abschluss der Promotion für ca. April/Mai 2026 erwartet wird. Neben einer Publikation zum gemeinsamen Forschungsthema mit Dr. Kluczniak (siehe Publikationsliste) hat der Doktorand mittlerweile eine zweite Publikation zu diesem Themenbereich gemeinsam mit seinem neuen Betreuer vorbereitet und reicht sie in Kürze ein.

2.2 Anwendungsmöglichkeiten

Die Forschungsergebnisse der Teilnehmenden des CSC-Programms werden vollumfänglich durch hochrangige Publikationen der internationalen Forschungsgemeinschaft zugänglich gemacht. Insbesondere auf international einschlägigen Konferenzen für IT-Sicherheit können die Teilnehmenden den Stand der Wissenschaft in ihrem jeweiligen Gebiet dadurch nachhaltig prägen und weiterentwickeln. Die von ihnen erzielten Forschungsergebnisse werden dadurch für Wissenschaftler:innen auf der ganzen Welt nutzbar gemacht.

Auch eine Vermittlung der Forschungserkenntnisse des CSC in die Industrie, Gesellschaft und Politik findet statt, und zwar im Wege des Technologietransfers oder über die Aus- und Weiterbildung von Studierenden und Akademiker:innen, etwa innerhalb der universitären Studiengänge in Cybersicherheit oder im Rahmen von Weiterbildungsmaßnahmen, an denen das CISPA beteiligt ist. Regelmäßig diskutiert das CISPA den Stand der Forschung im Bereich Informationssicherheit auch mit Politik und Gesellschaft, um einerseits Aufklärung zu betreiben und zu informieren und um andererseits wertvolles Feedback zur gesellschaftlichen Relevanz seiner Forschung zu erhalten.

Die von Dr. Kluczniak erforschten FHE-Methoden verfügen in der Tat über zahlreiche praxisrelevante Anwendungsmöglichkeiten in der Kryptographie, der Informationssicherheit, der Medizin, dem Marketing, dem Finanzsektor und vielen anderen Branchen. FHE-Methoden bilden die Grundlage für ein eigenes Geschäftsfeld, da sie Themen von der Theorie der Kryptographie, Computeralgebra und Algorithmen bis hin zum Entwurf von Compilern, Sprachen und Hardwarebeschleunigern abdecken. Gängige Anwendungen von FHE sind im Folgenden beispielhaft aufgeführt, um die Funktionalität von FHE zu veranschaulichen, wobei FHE-Methoden grundsätzlich sehr vielseitig sind und daher zahlreiche weitere Anwendungsfelder bestehen:

- Kollaborative Statistik für verschiedene Arten von Daten, einschließlich medizinischer und finanzieller Daten. Beispielsweise kann man FHE zur Erkennung von Finanzbetrug einsetzen, indem man Daten von verschiedenen Banken analysiert, ohne dass diese jemals Informationen an ihre Kunden weitergeben.
- Gemeinsames Training von Modellen für maschinelles Lernen. So können beispielsweise verschlüsselte Anzeigendaten von verschiedenen Nutzern gesammelt und Anzeigenprofile anhand der gemeinsamen Daten trainiert werden.
- Inferenz von Modellen des maschinellen Lernens. Man könnte beispielsweise ein System zur Erkennung von Malware danach abfragen, ob eine URL schädlich oder harmlos ist, ohne dem System die URL bekanntzugeben. In ähnlicher Weise könnte man einen DNA-Klassifikator nach grundlegenden Informationen über eine DNA-Probe befragen, ohne die DNA-Probe dem Dienstanbieter offenzulegen.
- In der Kryptographie kann FHE zur Erstellung von Blindsignaturen, Schwellenwertkryptographie-Primitiven, Verschleierungsschemata, sicheren Zwei-Parteien-Protokollen, Protokollen zum Abrufen privater Informationen, Protokollen für private Mengenüberschneidungen, Ringsignaturen usw. verwendet werden.

Dr. Kluczniak hat im Laufe seiner Tätigkeit im CSC zahlreiche Algorithmen entwickelt, die in vielen Fällen die zuvor besten FHE-Verfahren übertroffen haben. Zudem hat er Prototypen dieser Algorithmen implementiert. Ein wichtiger Teil seiner Arbeit war die Entwicklung der Open-Source-Bibliothek „FHE-Deck“, in der die meisten der im Rahmen seiner Tätigkeit entwickelten Methoden enthalten sind (<https://github.com/fhe-deck>). Die Entwicklung der Bibliothek war entscheidend, um Erfahrungen zu sammeln und die Gestaltung der Algorithmen in der Realität zu verwurzeln. Derzeit ist die Bibliothek stabil, und einige Methoden erzielen bessere Parameter als die weltweite Konkurrenz. Als internationale Konkurrenten können die CONCRETE-Bibliothek, die von einem Startup namens ZAMA (Frankreich) entwickelt wurde, und Open-FHE, das von einem Startup namens Duality Technologies (USA) erstellt wurde, aufgeführt werden. Andere bedeutende FHE-Bibliotheken, die von IBM und Microsoft entwickelt wurden, unterstützen eine ältere Form von FHE. Daher wäre es aus technischer Sicht möglich, aus den von Dr. Kluczniak entwickelten FHE-Methoden ein Start-up oder ein Spin-off zu gründen oder eine Vermarktung der entwickelten Technologie durch deutsche und europäische Industrie- und Regierungspartnern zu initiieren. Es ist jedoch zusätzliche nicht-wissenschaftliche technische Arbeit zu leisten, um tatsächlich ein Endprodukt zu erzeugen. Die im Rahmen des Vorhabens geleistete Arbeit deckt das Ziel der Verwertbarkeit insofern ab, als dass in Deutschland eine erste Wissens- und Erfahrungsbasis mit FHE mit neuen wettbewerbsfähigen Algorithmen und Protokollen aufgebaut werden konnte, die das Potenzial zur Kommerzialisierung haben. Dabei könnte die von Dr. Kluczniak bereitgestellte Bibliothek als bedeutsamer Ausgangspunkt dienen.

Die von Dr. Kluczniak erzielten Ergebnisse sind aufgrund ihrer Ausrichtung auf praktische Implementierungen und Anwendungsfälle von hohem wirtschaftlichem Interesse. Seine wichtigsten Ergebnisse können in Form eines Demonstrators aufgezeigt werden, der das Potenzial und die Anwendbarkeit der Ergebnisse einem breiteren Publikum verdeutlicht. Im Einklang mit diesem Verwertungspotenzial hat Dr. Kluczniak eingeladene Vorträge über vollständig homomorphe Verschlüsselung gehalten. Dabei handelt es sich um verschiedene Plenarvorträge (z.B. für die polnische Bankenvereinigung), zu denen er als Experte auf dem Gebiet der FHE eingeladen wurde:

- Ring Signatures: Optimal Size, No Setup – from Standard Assumptions. Invited Talk at Wroclaw University of Science and Technology. Warsaw, Poland. 2018.
- Recent Developments in Fully Homomorphic Encryption Research. Invited Talk at the Cryptographic Seminar at Warsaw University. 2022.
- Current State of FHE Implementations. Meeting with Cyberagency. Saarbrücken 2022.
- Recent Developments in Fully Homomorphic Encryption Research. Central European Conference on Cryptography. Smolenice, Slovakia. 2022.
- Recent Developments in Fully Homomorphic Encryption Research. Invited Talk - Computer Security & Cybersecurity Challenges. Paris, France. 2022.
- Circuit Privacy for FHEW/TFHE Style Fully Homomorphic Encryption in Practice. King's College London. London, UK. 2023.
- Applications of Fully Homomorphic Encryption in the Financial Sector. Invited Talk at Polish Bank Association. Warsaw, Poland. 2023.
- Circuit Privacy for FHEW/TFHE Style Fully Homomorphic Encryption in Practice. Invited Talk at FHE.org meetup. Online. 2023.

Dr. Kluczniak hat seine Forschung auch in die universitäre Lehre eingebracht, insbesondere über die Betreuung einer Bachelorarbeit und durch folgende Lehrveranstaltungen sowie weitere Veranstaltungen (z.B. CISPAs Young Researcher Security Convention 2019 oder Lunch Talks der Stanford University):

- Seminar „Advanced Topics in Modern Cryptography“ im Sommersemester 2019 an der Universität des Saarlandes
- Seminar „Digital and Privacy-Preserving Signatures“ im Wintersemester 2021/22 (zusammen mit Dr. Lucjan Hanzlik) an der Universität des Saarlandes
- Seminar „Applied Multiparty Computation and Fully Homomorphic Encryption“ im Wintersemester 2022/23 an der Universität des Saarlandes

2.3 Kollaborationen

Dr. Kluczniak kooperierte während seiner Teilnahme am CSC-Programm intensiv mit anderen Forschenden des CISPAs, die ebenfalls in der Kryptographieforschung tätig sind, insbesondere Dr. Lucjan Hanzlik im Rahmen einiger gemeinsamer Forschungsarbeiten. Er arbeitete auch eng mit Forschenden der Ruhr-Universität Bochum (siehe Abschnitt 2.1) zusammen, woraus ein gemeinsames Paper mit Prof. Tim Güneysu entstand.

Er kooperierte und publizierte zudem mit Prof. Man Ho Au von der Computing-Abteilung der Hong Kong Polytechnique University (Hong Kong SAR, China) und zum anderen mit Prof. Guomin Yang vom Institut für Cybersicherheit und Kryptologie, School of Computing and Information Technology, University of Wollongong (Australien) im Rahmen des Forschungsthemas „Gegenannahmen gegen kryptographische Angriffe auf kryptographische Hardware“.

Auch mit der Wroclaw University of Science and Technology in Polen pflegte Dr. Kluczniak engen Kontakt, wodurch verschiedene gemeinsame Paper und auch ein Buchkapitel zum Thema „Pseudonymous Signature Schemes“ im Buch „Advances in Cyber Security: Principles, Techniques, and Applications“ entstand.

Nach seinem Aufenthalt an der Stanford University blieb Dr. Kluczniak im engen Austausch mit der Gruppe von Prof. Dan Boneh. Darüber hinaus etablierte er eine fruchtbare Kooperation mit Forschenden der Katholieke Universiteit (KU) Leuven und publizierte mit Leonard Schild zwei gemeinsame Paper.

3 Publikationsliste

Im Folgenden werden die von Dr. Kluczniak im Rahmen seiner Teilnahme am CSC-Programm veröffentlichten Forschungspaper dargestellt (in chronologischer Reihenfolge beginnend bei 2024 bis 2018):

- Kamil Kluczniak, Leonard Schild. FDFB²: Functional Bootstrapping via Sparse Polynomial Multiplication. IACR Cryptol. ePrint Arch. 2024.
- Johannes Mono, Kamil Kluczniak, Tim Güneysu. Improved Circuit Synthesis with Amortized Bootstrapping for FHEW-like Schemes. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2024.
- Kamil Kluczniak, Giacomo Santato. On Circuit Private, Multikey and Threshold Approximate Homomorphic Encryption. IACR Eprint 2023.
- Kamil Kluczniak, Leonard Schild. FDFB: Full Domain Functional Bootstrapping Towards Practical Fully Homomorphic Encryption. IACR Transactions on Cryptographic Hardware and Embedded Systems 2023.
- Kamil Kluczniak. Circuit Privacy for FHEW/TFHE-Style Fully Homomorphic Encryption in Practice. IACR Cryptology ePrint Archive 2022.
- Kamil Kluczniak. NTRU-v-um: Secure Fully Homomorphic Encryption from NTRU with Small Modulus. CCS 2022.
- Kamil Kluczniak. Lockable Obfuscation from Circularly Insecure Fully Homomorphic Encryption. Public Key Cryptography 2022.
- Lucjan Hanzlik, Kamil Kluczniak. Explainable Arguments. Financial Cryptography and Data Security 2022.
- Kamil Kluczniak. Witness Encryption from Garbled Circuit and Multikey Fully Homomorphic Encryption Techniques. IACR Cryptology ePrint Archive 2020.
- Lucjan Hanzlik, Kamil Kluczniak, Mirosław Kutylowski. CTRL-PACE: Controlled Randomness for e-Passport Password Authentication. Fundamenta Informaticae 2019.
- Kamil Kluczniak, Jianfeng Wang, Xiaofeng Chen, Mirosław Kutylowski. Multi-device anonymous authentication. International Journal of Information Security 2019.
- Mirosław Kutylowski, Jakub Lemiesz, Marta Slowik, Marcin Slowik, Kamil Kluczniak, Maciej Gebala. GDPR-Compliant Reputation System Based on Self-certifying Domain Signatures. ISPEC 2019.

- Przemyslaw Blaskiewicz, Lucjan Hanzlik, Kamil Kluczniak, Lukasz Krzywiecki, Mirosław Kutylowski, Marcin Slowik, Marta Wszola. Pseudonymous Signature Schemes. *Advances in Cyber Security* 2019.
- Michael Backes, Nico Döttling, Lucjan Hanzlik, Kamil Kluczniak, Jonas Schneider: Ring Signatures: Logarithmic-Size, No Setup – from Standard Assumptions. *EU-ROCRYPT* 2019.
- Lucjan Hanzlik, Kamil Kluczniak, Mirosław Kutylowski. CTRL-PACE: Controlled Randomness for e-Passport Password Authentication. *Fundam. Informaticae* 2019.
- Lukasz Krzywiecki, Kamil Kluczniak, Patryk Koziel, Nisha Panwar. Privacy-oriented dependency via deniable SIGMA protocol. *Comput. Secur.* 2018.
- Kamil Kluczniak, Lucjan Hanzlik, Jianfeng Wang. Efficient VLR group signatures for smart cards. *Int. J. Embed. Syst.* 2018.
- Kamil Kluczniak, Man Ho Au. Fine-Tuning Decentralized Anonymous Payment Systems based on Arguments for Arithmetic Circuit Satisfiability. *IACR Cryptol. ePrint Arch.* 2018.
- Mirosław Kutylowski, Lucjan Hanzlik, Kamil Kluczniak: Towards Practical Security of Pseudonymous Signature on the BSI eIDAS Token. *IACR Cryptol. ePrint Arch.* 2018.
- Michael Backes, Lucjan Hanzlik, Kamil Kluczniak, Jonas Schneider. Signatures with Flexible Public Key: A Unified Approach to Privacy-Preserving Signatures (Full Version). *IACR Cryptol. ePrint Arch.* 2018:
- Man Ho Au, Siu-Ming Yiu, Jin Li, Xiapu Luo, Cong Wang, Aniello Castiglione, Kamil Kluczniak. *Network and System Security - 12th International Conference, NSS 2018, Hong Kong, China, August 27-29, 2018, Proceedings. Lecture Notes in Computer Science* 2018.
- Michael Backes, Lucjan Hanzlik, Kamil Kluczniak, Jonas Schneider. Signatures with Flexible Public Key: Introducing Equivalence Classes for Public Keys. *ASIACRYPT* 2018.

CISPA-Stanford Center



FOR CYBERSECURITY

Projekt Stanford_2018

- Kurzbericht -

Zuwendungsempfänger:	CISPA - Helmholtz-Zentrum für Informationssicherheit gGmbH
Förderkennzeichen:	16KIS0927
Projektleitung:	Prof. Dr. Dr. h. c. Michael Backes / Dr. Theo Jäger
Laufzeit des Vorhabens:	01.09.2018-30.09.2024

Inhalt

1	Zielsetzung	3
2	Inhalt und Ergebnisse.....	3
3	Anwendungsmöglichkeiten.....	4
4	Fazit	4

1 Zielsetzung

Das CISPA-Stanford Center for Cybersecurity (CSC) wurde als Kooperation zwischen dem CISPA Helmholtz-Zentrum für Informationssicherheit in Saarbrücken und der renommierten Stanford University in Kalifornien/USA etabliert. Kernziel des CSC ist es, mit einem innovativen Qualifizierungskonzept exzellenten wissenschaftlichen Nachwuchs zu hochausgebildeten Fach- und Führungskräften für Forschung und Industrie in der Informationssicherheit zu entwickeln. Dadurch kann das CSC-Programm bedeutsam dazu beitragen, die Wettbewerbsfähigkeit von Europa und speziell des Standorts Deutschland im Zukunftsfeld der Cybersicherheit zu unterstützen. Das Qualifizierungsprogramm ist in drei Phasen strukturiert: Phase 1 als Postdoktorand:in am CISPA, um die erforderliche wissenschaftliche Selbständigkeit für die darauffolgende Phase zu erlangen; Phase 2 als Visiting Assistant Professor an der Stanford University, um das amerikanische Wissenschaftssystem kennenzulernen und das akademische Profil weiter zu schärfen; und Phase 3 als Nachwuchsgruppenleiter:in am CISPA, um den weiteren Karriereweg in verantwortungsvollen Positionen in Wissenschaft oder Industrie innerhalb von Deutschland bzw. Europa oder weltweit unmittelbar vorzubereiten.

2 Inhalt und Ergebnisse

Die erste Kohorte des CSC startete im Jahr 2017 mit vier Teilnehmenden, die sich dank der gesammelten Erfahrungen und erlangten Qualifikationen rasch und erfolgreich auf Führungspositionen in der Wissenschaft bewerben konnten. Die im Rahmen des vorliegenden Projekts geförderte zweite Kohorte ist im Jahr 2018 mit zwei Teilnehmenden gestartet. Dr. Hojoon Lee trat am 01.09.2018 in das Programm ein, erhielt aber bereits frühzeitig während Phase 1 ein attraktives Stellenangebot der Sungkyunkwan University in Südkorea über eine Position als Associate Professor am Department of Computer Science and Engineering.

Dr. Kamil Kluczniak trat am 01.09.2018 als Postdoktorand in das Programm ein und nahm am 01.09.2019 die zweijährige Phase als Visiting Assistant Professor an der Stanford University auf. Er kehrte am 01.10.2021 als Nachwuchsgruppenleiter ans CISPA zurück. Dr. Kluczniak befasste sich hauptsächlich mit praktischen Aspekten der sicheren Berechnung, wobei der Schwerpunkt auf Techniken der vollständig homomorphen Verschlüsselung (fully homomorphic encryption; FHE) lag. FHE ist eine Technik, die es ermöglicht, Daten zu verschlüsseln und den Chiffretext an einen nicht vertrauenswürdigen Server zu senden, der mit den verschlüsselten Daten eine beliebige Berechnung durchführen und das Ergebnis der Berechnung zurücksenden kann. Mit einem speziellen geheimen Schlüssel kann das Ergebnis der Berechnung des Servers dann effizient wiederhergestellt werden.

Dr. Kluczniak und seine Gruppe haben neue FHE-Techniken entwickelt, die den Stand der Technik in der Praxis deutlich übertroffen haben. Insbesondere haben sie eine Methode namens „Functional Bootstrapping“ generiert, die bei praktischen Berechnungen mit verschlüsselten Daten eine über 1.000-fache Beschleunigung gegenüber früheren Methoden erzeugt. Die Gruppe hat das erste praxistaugliche FHE-Schema eingeführt und implementiert, das zu einer nicht-trivialen Beschleunigung führte. Es wurden neue Bereinigungsverfahren entwickelt, um die Sicherheitseigenschaften von einfacher FHE durch den Schutz von Schaltkreisen zu ergänzen, was für Anwendungen von FHE bei sicheren Mehrparteienberechnungen von entscheidender Bedeutung ist. Darüber hinaus hat Dr. Kluczniak den Stand der Technik von Schwellenwert-FHE analysiert. In Zusammenarbeit mit der Ruhr-Universität Bochum wurde einer der ersten Compiler entwickelt, der in der Lage ist, in C++ geschriebenen Code zu einer

spezifischen Schaltung zu kompilieren, die über verschlüsselte Daten verarbeitet werden kann. Letztendlich wurden alle praktischen Ergebnisse implementiert und zur Demonstration in Form einer Open-Source-Bibliothek zur Verfügung gestellt.

3 Anwendungsmöglichkeiten

Die Forschungsergebnisse der Teilnehmenden des CSC-Programms werden durch hochrangige Publikationen der internationalen Forschungsgemeinschaft zugänglich gemacht. Auch eine Vermittlung in die Industrie und Gesellschaft findet statt, und zwar im Wege des Technologietransfers oder über die Aus- und Weiterbildung von Akademiker:innen. Regelmäßig diskutiert das CISPA den Stand der Forschung auch mit Politik und Gesellschaft.

Die von Dr. Kluczniak erforschten FHE-Methoden sind mit zahlreichen Anwendungsmöglichkeiten in der Kryptographie, der Informationssicherheit, der Medizin, dem Marketing, dem Finanzsektor und vielen anderen Branchen verbunden. FHE-Methoden bilden somit die Grundlage für ein eigenes Geschäftsfeld und sind in den letzten Jahren deutlich praxistauglicher geworden, was renommierte Unternehmen dazu veranlasst hat, umfangreiche Mittel und Aufmerksamkeit in die Entwicklung neuer und effizienter FHE-Techniken zu investieren. Die wichtigsten Forschungs- und Startup-Zentren befinden sich jedoch derzeit in den USA, Frankreich und Korea. In Deutschland gibt es hingegen einen Mangel an Expertise zu FHE in Forschung oder Industrie. Daher bestand das Hauptziel der Tätigkeit von Dr. Kluczniak darin, die erste Forschungsgruppe in Deutschland aufzubauen, die sich auf die Entwicklung neuer praxisrelevanter FHE-Methoden konzentriert. Die dabei erzielten Methoden sollen mit internationalen Technologien konkurrieren können und unterstützen damit den Erwerb von Fachwissen für eine mögliche Vermarktung und Anwendung der Technologie durch die Industrie und die Politik innerhalb Deutschlands.

Die von Dr. Kluczniak erzielten Ergebnisse sind aufgrund ihrer Ausrichtung auf praktische Implementierungen und Anwendungsfälle von hohem wirtschaftlichem Interesse. Aus technischer Sicht wäre es möglich, daraus ein Start-up oder ein Spin-off zu gründen oder eine Vermarktung der entwickelten Technologie durch deutsche und europäische Industrie- und Regierungspartnern zu initiieren. Es ist jedoch zusätzliche nicht-wissenschaftliche technische Arbeit zu leisten, um tatsächlich ein Endprodukt zu erzeugen. Die im Rahmen des Vorhabens geleistete Arbeit deckt das Ziel der Verwertbarkeit insofern ab, als dass in Deutschland eine erste Wissens- und Erfahrungsbasis mit FHE mit neuen wettbewerbsfähigen Algorithmen und Protokollen aufgebaut werden konnte, die das Potenzial zur Kommerzialisierung haben.

4 Fazit

Durch die Teilnahme am CSC-Programm erlangen die Forschenden eine wissenschaftliche Exzellenz, die sich z.B. in hochrangigen Forschungspublikationen und Auszeichnungen widerspiegelt. Sie gehen ein breites Spektrum an Kooperationen in Forschung und Industrie ein, die ihnen in den jeweiligen wissenschaftlichen Projekten zugutekommen. Dank der im CSC erlangten Qualifikation können sie sich erfolgreich auf Leitungspositionen in Wissenschaft oder Industrie bewerben, sowohl in Deutschland als auch im internationalen Kontext. Durch die fortbestehende Vernetzung auch über die Programmteilnahme hinaus entwickeln sich längerfristige Kontakte und dadurch Möglichkeiten für neue Kooperationen mit externen (insbesondere Forschungs-)Einrichtungen, an denen die Teilnehmenden des CSC ihre Anschlusspositionen erlangt haben. Das gemeinsame Programm zwischen dem CISPA und der Stanford University hat sich somit als fruchtbares Instrument der wissenschaftlichen Qualifizierung und Karriereförderung herausgestellt und etabliert.

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht
3. Titel CISPA-Stanford Center for Cybersecurity - Projekt Stanford 2018	
4. Autor(en) [Name(n), Vorname(n)] Prof. Dr. Dr. h.c. Michael Backes Dr. Theo Jäger	5. Abschlussdatum des Vorhabens 30.09.2024
	6. Veröffentlichungsdatum
	7. Form der Publikation Document Control Sheet
8. Durchführende Institution(en) (Name, Adresse) CISPA - Helmholtz-Zentrum für Informationssicherheit gGmbH	9. Ber.-Nr. Durchführende Institution
	10. Förderkennzeichen 16KIS0927
	11. Seitenzahl
12. Fördernde Institution (Name, Adresse) BMBF	13. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. DOI (Digital Object Identifier)	
17. Vorgelegt bei (Titel, Ort, Datum) BMBF, 31.03.2025	
18. Kurzfassung Das CISPA-Stanford Center förderte exzellenten Nachwuchs in der Cybersicherheit. Seit 2017 forschten Teilnehmende in Deutschland und den USA zu Kryptographie, Verwundbarkeiten und sicherer Softwarekompilierung. Die Forschungsergebnisse wurden als Open-Source-Bibliothek veröffentlicht und in hochrangigen Publikationen publiziert. Die Erkenntnisse fanden Anwendung in Industrie und Gesellschaft. CISPA engagiert sich im Technologietransfer und berät Politik und Wirtschaft. Dr. Kluczniak erforschte vollhomomorphe Verschlüsselung (FHE), die in Kryptographie, Medizin und Finanzsektor genutzt wurde. Während die USA, Frankreich und Korea führend waren, fehlte es in Deutschland an Expertise. Ziel war es, eine deutsche Forschungsgruppe aufzubauen, die international konkurrenzfähige FHE-Methoden entwickelte. Die praxisnahen Ergebnisse hatten wirtschaftliches Potenzial. Das CSC-Programm förderte Exzellenz und Karrierechancen und erwies sich als wertvolles Kooperationsmodell	
19. Schlagwörter Cybersecurity, Nachwuchsförderung, Erklärbarkeit von Kryptographie, Verwundbarkeitserkennung, Security, Deutsch-Amerikanische Zusammenarbeit.	
20. Verlag	21. Preis

Nicht änderbare Endfassung mit der Kennung 2650246-3

Document control sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) Veröffentlichung (Publikation)	
3. title CISPA-Stanford Center for Cybersecurity - Projekt Stanford 2018		
4. author(s) (family name, first name(s)) Prof. Dr. Dr. h.c. Michael Backes Dr. Theo Jäger	5. end of project 30.09.2024	
	6. publication date	
	7. form of publication Document Control Sheet	
8. performing organization(s) name, address CISPA - Helmholtz-Zentrum für Informationssicherheit gGmbH	9. originators report no.	
	10. reference no. 16KIS0927	
	11. no. of pages	
12. sponsoring agency (name, address) BMBF	13. no. of references	
	14. no. of tables	
	15. no. of figures	
16. DOI (Digital Object Identifier)		
17. presented at (title, place, date) BMBF		
18. abstract <p>The CISPA-Stanford Centre promoted excellent young talent in cyber security. Since 2017, participants in Germany and the USA have been researching cryptography, vulnerabilities and secure software compilation. The research results were published as an open-source library and publicised in high-ranking publications.</p> <p>The findings have been applied in industry and society. CISPA is involved in technology transfer and advises politics and business.</p> <p>Dr Kluczniak researched fully homomorphic encryption (FHE), which was used in cryptography, medicine and the financial sector. While the USA, France and Korea were leading the way, there was a lack of expertise in Germany. The aim was to establish a German research group that would develop internationally competitive FHE methods.</p> <p>The practical results had commercial potential. The CSC programme promoted excellence and career opportunities and proved to be a valuable cooperation model</p>		
19. keywords Cybersecurity, promotion of young talent, explainability of cryptography, vulnerability detection, security, German-American cooperation		
20. publisher	21. price	

Nicht änderbare Endfassung mit der Kennung 2650243-5