GERMAN-FRENCH JOINT CALL ON CYBERSECURITY

2019 EDITION

Effizientes MPC und Integration in eine Privacy-Preserving Cloud-Umgebung

Abschlussbericht des Teilvorhabens

Universität Stuttgart
Keplerstr. 7
70049 Stuttgart

CRYPTECS
Verbundnummer KIS6DFR008

Inhaltsverzeichnis

1. Ziele und Stand der Forschung bei Projektbeginn

Das Ziel der Universität Stuttgart innerhalb des Verbundprojekts CRYPTECS war es, Multi-Party-Computation (MPC) für den industriellen Einsatz, insbesondere für Anwendungen des Maschinellen Lernens (ML), verfügbar zu machen. Dies sollte durch eine Effizienzsteigerung von MPC selbst, durch die Kombination von MPC mit weiteren Technologien für Privacy-Preserving Computing (PPC-Technologien) und durch die Integration und Bereitstellung der resultierenden datensicheren Protokolle als wiederverwendbare Dienste innerhalb der Cloud-Plattform CRYPTECS erreicht werden.

1.1. Ziele des Teilvorhabens

Multi-Party-Computation (MPC) ermöglicht es mehreren Parteien, gemeinsam Berechnungen auf vertraulichen Eingabedaten durchzuführen, ohne dabei Informationen über diese Daten oder etwaige Zwischenergebnisse offenzulegen. Während MPC in zahlreichen Anwendungsbereichen Verwendung findet, wurde im vorliegenden Projekt der Schwerpunkt auf datenschutzkonformes maschinelles Lernen (Privacy-Preserving Machine Learning) mittels MPC gelegt.

Ein vorrangiges wissenschaftliches Ziel der Universität Stuttgart im Rahmen des CRYPTECS-Projekts bestand entsprechend in der Entwicklung neuartiger MPC-Protokolle, die den industriellen Einsatz – insbesondere im Kontext maschinellen Lernens – ermöglichen. Zu diesem Zweck sollten die zum Projektbeginn leistungsfähigsten MPC-Modelle gezielt für ML-Operationen optimiert werden, um deren Effizienz signifikant zu steigern und damit die Grundlage für eine breite industrielle Anwendbarkeit zu schaffen.

Neben der Verbesserung von MPC-Verfahren hat sich das Teilvorhaben der Universität Stuttgart zum Ziel gesetzt, die Integration von MPC mit anderen sicheren (sogenannten) PPC-Technologien wie Fully Homomorphic Encryption (FHE), Differential Privacy (DP) und Trusted Execution Environments (TEEs) zu untersuchen, um die jeweils unterschiedlichen Stärken in den Bereichen Sicherheit und Leistungsfähigkeit bestmöglich für sicheres maschinelles Lernen nutzbar zu machen.

Zur Demonstration der praktischen Leistungsfähigkeit der entwickelten MPC-Protokolle und resultierenden Integrationsmodule sollten gemeinsam mit den industriellen Projektpartnern ausgewählte Pilotanwendungen identifiziert und evaluiert werden.

1.2. Stand der Wissenschaft und Technik

MPC-Protokolle wurden erstmals von Yao [Yao86] für den Spezialfall von zwei Parteien eingeführt und in den Folgejahren schrittweise erweitert und verbessert (z. B. [Bea92]). Es dauerte jedoch bis Anfang der 2000er Jahre bis erste Implementierungen, wie Fairplay [MNPS04], entwickelt wurden und ein weiteres Jahrzehnt und zahlreiche theoretische Verbesserungen, z. B. [DPSZ12], bis diese effizient genug für erste einfache Anwendungen waren. Weitere Fortschritte der letzten Jahre führten zu ersten industriellen Anwendungen von MPC [ABL+18]. Trotz dieser Fortschritte waren die bei Projektstart besten MPC-Protokolle für sich gegenseitig misstrauende Parteien, nicht leistungsstark genug für die komplexen Anwendungen im Bereich des maschinellen Lernens. Hier setzte das Projekt der Universität Stuttgart an.

Die effizientesten MPC-Protokolle für Berechnungen beliebig vieler sich gegenseitig misstrauender Parteien bei Projektbeginn 2021 waren SPDZ [DPSZ12] und darauf aufbauende Protokolle wie [KPR18]. Diese nutzen ein Zweiphasenmodell bestehend aus einer Offline-Phase, in der (strukturierte) Zufallszahlen mit gewissen Eigenschaften von den teilnehmenden Parteien erzeugt und authentifiziert werden, und einer Online-Phase, in der diese strukturierten Zufallszahlen von den Parteien genutzt werden, um eine Berechnung auf geheimen Eingaben durchzuführen.

Die Offline-Phasen von [DPSZ12] und [KPR18] nutzen dabei das homomorphe Verschlüsselungsverfahren aus [BGV12] zur Erzeugung der strukturierten Zufallszahlen, sogenannte

Beavertripel. Dabei wählt jede Partei P_i zwei Zufallszahlen a_i und b_i in einem Kreisteilungsring über einem endlichen Körper. Die Summe a der a_i ist dann ebenso zufällig wie die Summe b der b_i und ist keiner der Parteien bekannt, denn jede Partei behält ihren Anteil für sich. Die Offline-Protokolle in [DPSZ12] und [KPR18] nutzen nun die lineare Struktur des BGV-Verschlüsselungsschemas, um jeder Partei ein c_i zu geben, sodass für die Summe c der c_i gilt: $ab = c$. Wird das Protokoll erfolgreich abgeschlossen, so kann sich jede ehrliche Partei sicher sein, dass niemand a, b oder c kennt, selbst dann, wenn alle anderen Parteien aktiv versucht haben, die Berechnungen zu manipulieren. In der Online-Phase werden die Beavertripel von den teilnehmenden Parteien verwendet, um mit minimaler Kommunikation multiplikative Operationen auszuführen.

Während die Offline-Phase aufwändig ist, viel Kommunikation zwischen den Parteien und eine hohe Bandbreite benötigt, ist die Online-Phase nahezu ideal. Die Verschiebung eines Großteils der Berechnungs- und Kommunikationskosten in die Offline-Phase stellt dabei nur selten ein Problem dar, da diese Berechnungen schon beginnen können, sobald die teilnehmenden Parteien bekannt sind und damit lange bevor die Berechnung auf den geheimen Eingabedaten startet. Die eigentliche Berechnung auf den geheimen Eingabedaten in der Online-Phase ist dann verhältnismäßig schnell.

Beavertripel sind universell einsetzbar und damit a priori nicht optimiert für spezielle Operationen. Tatsächlich haben [Dah19], [MZ17], [CKR+20] erkannt, dass für komplexere Operationen, wie die Matrizenmultiplikation, die etwa in datensicheren ML-Anwendungen häufig verwendet wird, geeignet strukturierte Zufallszahlen geringere Berechnungs- und Übertragungskosten liefern als der generische Ansatz mit Beavertripeln. Solche verallgemeinerten Tripel erzeugen Matrizen A, B und C mit $AB = C$ mittels Matrizenmultiplikation. Überraschenderweise können mit diesen neuen Matrixtripeln sowohl die Offline- als auch die Online-Phase optimiert werden. Vergleichbare Konstruktionen existieren bei Projektbeginn bereits für die in ML häufig verwendeten Faltungen, jedoch nicht für Polynomevaluationen in Aktivierungsfunktionen. Unsere Projekt liefert hier neue Ansätze und verbessert alle oben genannten in ML zentralen Berechnungen in der Online- und Offlinephase.

Ein weiteres Hauptziel des Teilprojekts der Universität Stuttgart ist die erfolgreiche Integration von MPC mit anderen PPC-Technologien, wie lokale und globale Differential Privacy (LDP und GDP), homomorphe Verschlüsselung (HE und FHE) sowie Trusted Execution Environments (TEEs). Während die Forschung auch in diesen Forschungszweigen in den letzten Jahren stark vorangeschritten ist, gibt es bisher nur sehr wenige Ergebnisse zur Integration der verschiedenen Technologien wie z. B. [KOV15] und [All19]. Deshalb mussten für die Integration von MPC mit diesen TPPC-Technologien komplett neue datensichere Lösungen gefunden werden.

2. Durchgeführten Arbeiten im Vergleich zur ursprünglichen Vorhabenbeschreibung

2.1. Arbeitspakete der Teilvorhabensbeschreibung

Im Folgenden sollen die Arbeiten an den einzelnen Arbeitspaketen des Teilprojekts der Universität Stuttgart beschrieben werden. Die Nummerierung orientiert sich an der entsprechenden Teilvorhabensbeschreibung. Neben der Darstellung der eigentlichen wissenschaftlichen Ergebnisse werden Änderungen in der zeitlichen Abfolge und beim Personaleinsatz erläutert. Etwaige Änderungen wurden auch bereits in den Zwischenberichten aufgeführt.
Für Arbeitspakete, die entsprechend der Teilvorhabensbeschreibung durchgeführt wurden, wird der Personaleinsatz nicht weiter ausgeführt. Zusätzlich wurden während der Projektarbeit entstandene (uns bekannte) Arbeiten bei anderen Stellen den jeweils relevanten Arbeitspaketen zugeordnet.

AP-Nr. / Titel	2.1 Sicherheitsmodelle
Bearbeitungszeitraum	M1-M2, M20
Gesamtumfang	4,0 Personenmonate (2 PM Postdoc, 2PM Doktorand)
Ziele des Arbeitspaketes	
❖ Analyse von Pilotanwendungen bezüglich Sicherheitsaspekten ❖ Entwicklung von MPC-Modellen zur Realisierung der Pilotanwendungen	

Das Arbeitspaket sollte zu Projektbeginn in den Monaten 1 und 2 (M1, M2) und später in M20 mit insgesamt 4 Personenmonaten die Einsatzmöglichkeit von MPC für Pilotanwendungen der Industriepartner analysieren. Leider war mit Projektbeginn eine Beschreibung der Pilotanwendungen der Industriepartner Bosch und Orange noch nicht verfügbar. Im ersten Projektjahr vorgestellte Pilotanwendungen, wie beispielsweise im Bereich der Geo-Indistinguishability mobiler Endgeräte (Orange) oder im Smart-Home-Bereich (Robert Bosch GmbH), wurden von uns für den Einsatz von MPC analysiert und mit den Projektpartnern zunächst weiterentwickelt. Beide Projekte wurden jedoch in den späteren Projektjahren von den Industriepartnern nicht weiterverfolgt. Stattdessen wurden neue Pilotprojekte entwickelt:

(1) Identifizierung bösartiger URL-Aufrufe bei Telekommunikationsroutern mittels maschinellen Lernens (Orange),
(2) Analyse des E-Mail-Verkehrs in Großunternehmen (Orange),
(3) Mitarbeiterstatistiken im Bereich Human Resources (Robert Bosch GmbH).

Auch für diese Pilotprojekte wurde die Anwendbarkeit von MPC analysiert. Während (1) nach ersten erfolgreichen Tests unserer neu entwickelten MPC-Protokolle aufgrund personeller Umstellungen beim Projektpartner nicht weiterverfolgt werden konnte, wird (2) zur Evaluation unseres Kooperationsprojekts mit INRIA und Orange (siehe AP 4.3 und [14]) verwendet. Im Pilotprojekt (3) kommen mit der von Bosch entwickelten Carbyne-Stack-Plattform [Car21] aktiv-sichere MPC-Protokolle mittels MP-SPDZ [MP-SPDZ] zum Einsatz. Carbyne-Stack stellt dabei eine Cloudinfrastruktur zur Verfügung die automatisch Protokolle aus MP-SPDZ einbindet. MP-SPDZ enthält die Implementierung vieler der schnellsten MPC-Protokolle wie aus [DPSZ12] oder [KPR18]. Von der Universität Stuttgart in diesem Projekt entwickelte MPC-Protokolle und ihre Implementierungen (siehe AP 3.1 – AP 3.3 unten) sind Erweiterungen von MP-SPDZ und somit in Carbyne Stack und für die Pilotanwendung (3) verwendbar.

Aufgrund der zwischenzeitlichen Änderung der Pilotanwendungen fanden die Arbeiten an AP 2.1 nach dem jeweiligen Bekanntwerden der neuen Pilotanwendungen durch die Projektpartner statt.

AP-Nr. / Titel	3.1 Matrixoperationen
Bearbeitungszeitraum	M1-M7, M15-M29
Gesamtumfang	5,0 Personenmonate (2 PM Postdoc, 3 PM Doktorand)
Ziele des Arbeitspaketes	
❖ Protokoll zur Generierung von Matrizentripel mit linearer homomorpher Verschlüsselung (LHE) in der MPC Offline-Phase ❖ Bestimmung idealer Sicherheitsparameter für die aktive Sicherheit der neuen Offline-Phase ❖ theoretische Analyse der Leistungsfähigkeit der Matrizentripelgenerierung im Vergleich zu der bisher effizientesten Generierung ❖ generische Implementierung von Matrizentripeln ❖ technischer Report zum Forschungsinhalt des Arbeitspakets	

Das Arbeitspaket war ab Projektbeginn geplant. In der tatsächlichen Abfolge wurde jedoch das Arbeitspaket AP 3.3 (siehe unten) vorgezogen, entsprechend hat sich die Hauptarbeit an AP 3.1 um 8 Monate auf M9–M12 verschoben. Der personelle Aufwand blieb dabei gleich.

Matrizentripel (A.3.1) verallgemeinern klassische Beavertripel und optimieren Matrizenmultiplikationen in MPC-Protokollen mit Offline- und Onlinephase. Entsprechend unserer Vorhabensbeschreibung wurde zunächst die effiziente Generierung von Matrizentripeln mit einer linear-homomorphen Offlinephase erforscht. Hierbei wurden über den Antrag hinausgehende Fortschritte erreicht:

(1) Für linear-homomorphe Offlinephasen wurde ein neuer Sicherheitsansatz entwickelt. Dabei werden die Generierung der eigentlichen Tripel und die Authentifizierung miteinander verknüpft. Durch diese Verknüpfung werden bisher notwendige zusätzliche Sicherheitsprotokolle („Sacrificing“) überflüssig. Diese Optimierung verringert sowohl die Laufzeit als auch die Menge an Daten, die zwischen den Parteien ausgetauscht werden muss, d. h. die Bandbreite. Das Ergebnis gilt zudem nicht nur für Matrizenoperationen, sondern allgemein für Multiplikationen in beliebigen Ringen. Insbesondere können damit auch die zentralen (und immer noch am häufigsten in MPC-Protokollen verwendeten) Beavertripel effizienter generiert werden.
(2) Für spezielle Matrizenoperationen, z. B. die Quadrierung von Matrizen oder die Auswertung von Skalarprodukten, wurde eine neue Form von Matrizentupeln gefunden, die schneller in der Offlinephase generiert werden können und die zusätzlich auch die zeitkritische Onlinephase verbessern.

Entsprechend (A.3.1.2, A.3.1.3) wurde die Sicherheit aller neuen Protokolle formal bewiesen. Für Matrizen wurde die notwendige Anpassung der Sicherheitsparameter bestimmt: Eine Vergrößerung der Bitlänge um die Bitlänge der Matrizendimensionen ist notwendig, um die Sicherheit der Protokolle zu garantieren. Zum Beispiel werden zusätzlich 10 Bits für 1024-dimensionale Matrizen benötigt. Für übliche Matrizendimensionen hat die dadurch größere Bitlänge nur einen kleinen negativen Einfluss auf die Laufzeit. Die Vorteile des Matrizentripelansatzes überwiegen diesen Nachteil deutlich. Alle neuen Protokolle wurden sowohl für Körperoperationen (Beavertripel) als auch Matrizenoperationen (Matrizentupel) als Erweiterung der zurzeit effizientesten aktiv-sicheren MPC-Plattform [MP-SPDZ] implementiert (A.3.1.5, A.3.1.6) und sind somit mit der CarbyneStack-Plattform [Car21] der Projektpartner nutzbar. Sowohl der theoretische (A.3.1.4) als auch der tatsächliche Vergleich mit den bisher besten Protokollen für Beavertripelgenerierung ([KPR18] mit TopGear) und Matrizentripelgenerierung ([CKR+20]) zeigt einen klaren Vorteil unserer Ergebnisse sowohl bei Laufzeit als auch bei Bandbreite. Beispielhaft erhalten wir eine 33 % kleinere Bandbreite bei der Beavertripelgenerierung als [KPR18] und eine 39 % kleinere Bandbreite bei der Matrizentripelgenerierung als [CKR+20] im 2-Parteien-Setup. Für spezielle Operationen sind die Vorteile noch größer. In einfachen Anwendungen des maschinellen Lernens (ML) sparen wir 28 %–74 % in der Laufzeit und 57 %–66 % in der Bandbreite.

Zusätzlich erwarten wir, dass sich unser Ansatz ohne Sacrificing mit kürzlich erschienenen SPDZ-Verbesserungen wie Coral [Hua+24] kombinieren lässt und die Protokolle damit verbessert werden können.

Die Ergebnisse wurden bei der Top-Konferenz „ASIA Conference on Computer and Communications Security“ (AsiaCCS 2023) eingereicht, akzeptiert und im Juli 2023 auf der Konferenz präsentiert. Die Ergebnisse sind als [4] in den Proceedings zur Konferenz veröffentlicht. Eine Erweiterung von [4] wurde als [8] beim “Theory and Practice of Multi-Party Computation Workshop” (TPMPC'24) angenommen und präsentiert.

AP-Nr. / Titel	3.2 Tensoroperationen
Bearbeitungszeitraum	M8-M12, M15-M29

Gesamtumfang	4,5 Personenmonate (4,5 PM Doktorand)
Ziele des Arbeitspaketes	
❖ Generierung von Tensortripeln mit LHE in der MPC-Offline-Phase ❖ Bestimmung idealer Sicherheitsparameter für aktive Sicherheit der neuen Offline-Phase ❖ theoretische Analyse der Leistungsfähigkeit der Tensortripelgenerierung im Vergleich mit der bisher effizientesten bekannten Generierung ❖ Online-Phase auf Basis von Tensortripeln ❖ technischer Report zum Forschungsinhalt des Arbeitspakets ❖ generische Implementierung von Tensortripeln	

Das Arbeitspaket AP 3.2 war vorrangig in den Monaten M8–M12 geplant. Entsprechend AP 3.1 wurde auch AP 3.2 um 6 Monate auf M12–M16 verschoben.

Tensortripel (A.3.2) sind (ähnlich wie Matrizentripel) speziell konstruierte strukturierte Zufallszahlen, die Tensorfaltungen beschleunigen. Auch in diesem Teilprojekt wurde zunächst die Generierung der Tripel erforscht. Hierbei konnte neben der ursprünglich geplanten Generierung mittels linear-homomorpher Verschlüsselung LHE (wie in A.3.2.1) zusätzlich auch eine Generierung mit SHE (somewhat homomorphic encryption) konstruiert werden, die für MPC-Protokolle mit vielen Parteien eine bessere Effizienz liefert. Im Rahmen von AP 4.5 (siehe unten) wurden neue Packmethoden für homomorphe Verschlüsselungssysteme entwickelt, die genutzt werden können, um MPC-Berechnungen zu beschleunigen. Mithilfe dieser Packmethoden können mit sehr wenigen Chiffretextoperationen viele Tensortripel gleichzeitig erzeugt werden. Dies führt zu einer hohen Effizienz unserer Protokolle. Die Verwendung von Packmethoden und Tensortupeln führt jedoch zu einer längeren Bitlänge (A.3.2.3). Um diesem negativen Effekt entgegenzuwirken, wurde eine neue Methode entwickelt, große Tensorfaltungen in kleinere aufzuspalten, sodass der Anstieg der Bitlänge moderat bleibt. Wir beweisen die Sicherheit aller Protokolle gegen eine Mehrheit aktiver Angreifer formal (A.3.2.2, A.3.2.3).

Weiterhin wurden alle neuen Protokolle als Erweiterung von [MP-SPDZ] implementiert (A.3.2.5) und sind somit mit der CarbyneStack-Plattform [Car21] der Projektpartner nutzbar. Sowohl die theoretische Analyse (A.3.2.4) als auch der Laufzeitvergleich zeigen einen klaren Vorteil unserer neuen Konstruktion. Beispielhaft erhalten wir eine um den Faktor 3,01 (WAN) bis 4,82 (LAN) schnellere Offlinephase für den ML-Algorithmus ResNet-50 im Vergleich mit [KPR18]. In der Onlinephase erhalten wir Beschleunigungen um Faktoren 40,15 (LAN) und 41,84 (WAN).
Bei Projektende ist unser Protokoll damit das schnellste aktiv-sichere Protokoll zur Berechnung von Tensorfaltungen gegen hochgradig bösartige Angreifer. Die Optimierung von Tensorfaltungen in MPC bleibt jedoch ein hochaktives Forschungsgebiet, in dem neuere Ergebnisse wie [LW24], [WHZ24], [HBA24] sich auf spezielle Typen von Faltungen und Anwendungen fokussieren.

Unsere Ergebnisse wurden auf der Top-Konferenz "Privacy Enhancing Technologies Symposium" (PETS 2023) präsentiert und veröffentlicht [5]. Darüber hinaus erhielt unser Artikel einen **zweiten Preis des Andreas Pfitzmann Best Student Awards**. Teile der Ergebnisse sind zudem in [8] eingeflossen. Zusätzlich wurde die Implementierung [22] getrennt begutachtet und als Softwareartifact zu PETS 2023 angenommen.

AP-Nr. / Titel	3.3 Polynomiale Operationen
Bearbeitungszeitraum	M7-M29
Gesamtumfang	8,5 Personenmonate (6 PM Postdoc, 2,5 PM Doktorand)
Ziele des Arbeitspaketes	

- ❖ Protokoll zur sicheren Generierung polynomialer Tupel
- ❖ optimierte polynomiale Tupel von kleiner Tupelgröße
- ❖ Integration polynomialer Tupel in ML
- ❖ generische Implementierung polynomialer Tupel

Das Arbeitspaket AP 3.3 war ab Monat M7 geplant. Abweichend von der ursprünglichen Planung wurde TVB A.3.3 auf M1 vorgezogen, statt Matrix- und Tensoroperationen (TVB A.3.1 und TVB A.3.2), welche stattdessen anschließend behandelt wurden (siehe oben).

Für polynomiale Operationen konnten schnell Tupel strukturierter Zufallszahlen konstruiert werden, die eine aktiv-sichere Berechnung polynomialer Operationen zulassen (TVB A.3.3.1), d. h. insbesondere können auch bösartige Parteien keine Informationen über die sensiblen Daten ehrlicher Parteien erlangen. Die Sicherheit der neuen Konstruktion wurde formal bewiesen: Die Auswertung auf sensiblen Daten in der Onlinephase ist dabei informationstheoretisch sicher, die Konstruktion der strukturierten Tupel ist statistisch sicher, d. h. insbesondere unabhängig von der Leistungsfähigkeit eines Angreifers. Wie bereits im Arbeitsplan angedeutet, führt die starke Verlagerung des Rechenaufwandes in die Offlinephase zwar zu einer sehr effizienten Onlinephase, aber auch zu einer sehr aufwendigen Offlinephase. Die Offlinephase ist oft nicht zeitkritisch, was diese Verlagerung in der Regel rechtfertigt. Die in TVB A.3.3.1 konstruierten polynomialen Tupel führen unter ungünstigen Umständen jedoch zu einer exponentiellen Erhöhung des Rechenaufwandes, was diese Tupel in diesen Fällen unbrauchbar macht. Der Forschungsschwerpunkt lag im Folgenden deshalb auf der Reduktion der Tupelgröße entsprechend TVB A.3.3.3. Als Ergebnis konnten neue (von uns polynomiale Tupel genannte) strukturierte Zufallszahlen konstruiert werden, die weitaus flexibler sind als in TVB A.3.3.3 angenommen. Unsere MPC-Protokolle werden dadurch vielseitiger und effizienter anwendbar bei gleichen Sicherheitsgarantien.

Um den Vorteil polynomialer Tupel über die in TVB A.3.3.1 konstruierten Tupel sowie die Vergleichsliteratur zu zeigen, wurde eine Implementierung der Onlinephase erstellt (TVB A.3.3.6). Diese basiert auf [MP-SPDZ] und ist somit mit der CarbyneStack-Plattform [Car21] der Projektpartner nutzbar. Sowohl Evaluierungen generischer Operationen als auch Anwendungsbeispiele im Bereich des maschinellen Lernens bestätigen die Vorteile unseres neuen Ansatzes gegenüber den besten bisher existierenden Implementierungen wie MP-SPDZ. Zusätzlich wurden polynomiale Tupel auch für nicht-arithmetische Operationen, wie Vergleichsoperationen, nutzbar gemacht – auch hier ergibt sich ein klarer Vorteil des neuen Ansatzes. Damit lassen sich mit Polytupeln weitere Komponenten von ML-Algorithmen wie Argmax/ReLU effizienter in MPC realisieren, was die Gesamtlaufzeit der ML-Anwendungen entsprechend weiter verringert. Die Anwendung über Vergleichsoperationen ist zudem unabhängig von der Fixpunktgenauigkeit, was die Polytupel unabhängig von den Ergebnissen in AP 3.4 (siehe unten) einsetzbar macht.

Unsere Ergebnisse wurden auf der Top-Konferenz Asiacrypt 2024 präsentiert und als [12] veröffentlicht. Zusätzlich wurde die Implementierung [24] getrennt begutachtet und als Softwareartifact zu Asiacrypt 2024 angenommen. Zudem sind die im Rahmen von [12] konstruierten binomialen Tupel (ein Spezialfall unserer polynomialen Tupel) bereits in https://eprint.iacr.org/2025/675 aufgegriffen worden.

AP-Nr. / Titel	3.4 Fixpunktoperationen
Bearbeitungszeitraum	M16-M29
Gesamtumfang	6,0 Personenmonate (6 PM Doktorand)
Ziele des Arbeitspaketes	
❖ Definition von Tupeln kompatibel mit Fixpunktoperationen ❖ formale Sicherheitsbeweise der Fixpunktprotokolle ❖ Integration von Fixpunkttupeln in ML-Modelle	

❖ Implementierung von Fixpunkttupeln

Eingabedaten im Rahmen von maschinellem Lernen fallen zumeist als reelle Zahlen an, die sich zum Beispiel mit einer gewissen Genauigkeit als Fixpunktzahlen speichern lassen. MPC-Protokolle sind dagegen oftmals auf der algebraischen Struktur endlicher Körper und Ringe aufgebaut. Um die Berechnung auf reellen Zahlen mittels MPC durchzuführen, wird die Fixpunktzahl als eine ganze Zahl dargestellt, indem der Dezimalpunkt entfernt wird, d. h. wir multiplizieren mit einer ausreichend großen Basispotenz, damit das Ergebnis ganzzahlig wird. Anschließend wird die MPC-Berechnung durchgeführt und im Ergebnis der Dezimalpunkt wieder eingefügt. Gerade bei multiplikativen Operationen führt dies zu Problemen, z. B. $1{,}1 \cdot 1{,}3$ wird als $11 \cdot 13 = 143$ berechnet, der Dezimalpunkt muss also so gesetzt werden, dass zwei Nachkommastellen entstehen, um 1,43 zu erhalten. Auch werden die Zahlen schnell sehr groß, sodass sie bald die Grenze des endlichen Rings übersteigen und damit die Information zerstören. Beispielsweise ist $143 \bmod 100 = 43$ und damit nicht mehr äquivalent zu 1,43.

Wie in der Teilvorhabensbeschreibung ausgeführt, sind die in AP 3.3 entwickelten strukturierten Zufallszahlen (sowohl aus A.3.3.1 als auch unsere polynomialen Tupel) nicht natürlich mit Fixpunktdarstellungen kompatibel. Überraschenderweise liefert, wie oben bereits beschrieben, der polynomiale Tupelansatz jedoch bereits die Möglichkeit für ML-Anwendungen (bzw. genauer für die Evaluierung von Aktivierungsfunktionen)**,** das Fixpunktproblem zu umgehen, indem statt polynomialer Approximationen glatter Aktivierungsfunktionen (wie Softmax), vergleichsbasierte Aktivierugsfunktionen wie Argmax oder ReLU verwendet werden. Dieser Ansatz wurde als Erweiterung von AP 3.3 bzw. [24] bereits implementiert und die resultierende Effizienzsteigerung in [12] beschrieben.

Für AP 3.4 wurde deshalb auf eine Implementierung (AP 3.4.5 und AP 3.4.6) verzichtet. Die Arbeitsabschnitte AP 3.4.1–AP 3.4.4 wurden jedoch in leicht reduziertem Umfang mit 3,0 PM durchgeführt. Sie bleiben weiterhin relevant für Anwendungen, z. B. außerhalb von ML, wo die Auswertung von Polynomen auf Fixpunkten nicht ersetzt werden kann. Insbesondere wurden in AP 3.4.2 neue Fixpunkttupel entwickelt, die die Generierung (leicht modifizierter) polynomialer Tupel in der Offlinephase ermöglichen, sodass die Genauigkeit der Onlineberechnungen auf sensiblen Daten gewährleistet ist und ein Overflow verhindert wird.

Die Ergebnisse wurden in einem technischen Bericht [18] zusammengefasst und werden zurzeit für die Veröffentlichung auf einer Fachkonferenz vorbereitet.

Die in AP 3.4 frei gewordenen Personenmonate wurden im neuen Arbeitspaket zu MPC über Grundringen der Charakteristik 2 (siehe unten und [7]) genutzt.

AP-Nr. / Titel	4.1 Integrationsschemata
Bearbeitungszeitraum	M13-M17
Gesamtumfang	3,5 Personenmonate (3,5 Postdoc)
Ziele des Arbeitspaketes	
❖ Integrationsschemata für MPC, LDP, GDP, TEEs, HE	

Das Arbeitspaket sollte Integrationsschemata für PPC-Technologien im Rahmen einer Cloudplattform untersuchen. Dabei wurde eine neue Integrationsmöglichkeit von MPC und DP entwickelt (siehe AP 4.3). Weiterhin wurden bekannte Integrationsmethoden von TEEs und MPC sowie homomorpher Verschlüsselung und MPC auf die in AP 3.1–AP 3.3 antragsgemäß entwickelten Protokolle erweitert.

Aufgrund der zusätzlichen Arbeit an [7] (siehe neue Arbeitspakete unten) und der Arbeit an [5] im Rahmen von AP 4.5 hat sich die Arbeit an AP 4.1 um ca. 3 Monate verschoben.

AP-Nr. / Titel	4.2 Sicherheits- und Auswertungsmetriken
Bearbeitungszeitraum	M18-M23
Gesamtumfang	4,0 Personenmonate (4 PM Postdoc)
Ziele des Arbeitspaketes	
❖ Sicherheits- und Auswertungsmetriken für integrierte Systeme von PPC-Technologien	

Während Sicherheitsdefinitionen für einzelne PPC-Technologien existieren und allgemein akzeptiert sind, gibt es für integrierte Systeme im Allgemeinen keine Sicherheitsmetriken, die den Schutz privater Daten in integrierten Systemen verschiedener PPC-Technologien quantifizieren und damit messbar machen. Entsprechend wurde für das in AP 4.1 neu entwickelte Integrationsschema von MPC und Differential Privacy (DP) ein neuer Sicherheitsbegriff (AP 4.2.2) eingeführt, der Differential Privacy für eine gegebene Verteilung der Inputdaten eines Protokolls liefert (siehe 4.3 für Details). Der neue Sicherheitsbegriff ist in natürlicher Weise mit MPC-Berechnungen kompatibel, sodass sich die Sicherheitsgarantien der eingesetzten MPC-Protokolle auf das integrierte System übertragen. Darüber hinaus liefert er für die CRYPTECS-Pilotanwendung (cf. (2) in AP 2.1) zudem die Standard-Differential-Privacy des integrierten Systems.

Entsprechend AP 4.1 wurde auch AP 4.2 um 3 Monate verschoben.

AP-Nr. / Titel	4.3 Integration von LDP und MPC
Bearbeitungszeitraum	M24-M28
Gesamtumfang	5,5 Personenmonate (3 PM Postdoc, 2,5 PM Doktorand)
Ziele des Arbeitspaketes	

Im Laufe des Projektes hat sich die Integration von MPC und lokaler und globaler Differential Privacy als vielversprechendster Lösungsansatz für die Pilotanwendung (2) des Industriepartners Orange herausgestellt (siehe AP 2.1). Als multinationaler Konzern besteht die Unternehmensgruppe aus dem Mutterkonzern Orange und ungefähr 80 kleineren Tochterunternehmen (TUs). Während die Unternehmensgruppe ein gemeinsames wirtschaftliches Interesse verbindet, sind die einzelnen Tochtergesellschaften teilweise rechtlich unabhängig. Der Austausch von Daten zwischen den Tochtergesellschaften und Orange unterliegt damit im Allgemeinen der Datenschutz-Grundverordnung (DSGVO). Insbesondere können beispielsweise Mitarbeiterdaten nicht an den Mutterkonzern weitergegeben werden. Im konkreten Anwendungsfall sucht Orange eine Methode, konzernübergreifende Statistiken zur E-Mail-Kommunikation innerhalb der Firmengruppen zu erhalten, ohne dass dabei das Kommunikationsverhalten einzelner Mitarbeiter bekannt wird.
Mittels MPC können die verschiedenen TUs sowohl ihre lokalen Statistiken kombinieren als auch mittels globaler Differential Privacy so verschleiern, dass die Orange zur Verfügung gestellten Ergebnisse keine relevanten Informationen über die TU-interne Statistik preisgeben. Während diese generische Kombination von GDP und MPC funktioniert, konnten wir zeigen, dass die resultierende Verschleierung und der damit einhergehende Genauigkeitsverlust für nahezu alle Anwendungen unnötig groß ist. Ähnlich verhält es sich mit Kombinationen von MPC und lokaler Differential Privacy (LDP), bei der jeder Mitarbeiter selbst sein Kommunikationsverhalten verschleiert.

Wir haben deshalb einen neuartigen Ansatz gewählt, bei dem jedes Tochterunternehmen, abhängig von der ihm zur Verfügung stehenden Privacy-Budget, eine Verschleierung so wählt, dass die Summe aller

Verschleierungen unter MPC gerade ausreicht, um das Kommunikationsverhalten eines einzelnen Mitarbeiters zu schützen und dabei eine möglichst genaue Statistik liefert.
Dazu definieren wir (entsprechend AP 4.2) den neuen Begriff der Differential Privacy unter einer gegebenen Inputverteilung und zeigen, dass der neue Sicherheitsbegriff in natürlicher Weise klassische Sicherheitsbegriffe in MPC und Differential Privacy in unserem Setup verallgemeinert. Wir präsentieren einen neuen Verschleierungsmechanismus und zeigen, dass er der neuen Sicherheitsdefinition genügt (AP 4.3.2). Weiterhin haben wir den neuen Mechanismus implementiert und auf die Pilotanwendung von Orange angewendet (AP 4.3.3). Unsere Evaluation zeigt, dass der neu entwickelte Mechanismus deutlich genauere Statistiken liefert als vergleichbar generische Kombinationen von MPC und Differential Privacy (GDP oder LDP), bei gleichbleibender Sicherheit.

Unsere Ergebnisse [14] sind zurzeit unter Begutachtung bei der Top-Konferenz „Computer Security Foundations Symposium (IEEE CSF)“.

Aufgrund der Verschiebung der Arbeitsinhalte zur Integration von GDP und MPC aus AP 4.4 nach AP 4.3 hat sich der Arbeitsaufwand für AP 4.3 um 3,5 Monate auf insgesamt 9 PM erhöht (5 PM Postdoc, 4 PM Doktorand). Die Arbeit an AP 4.3 und AP 4.4 hat sich aufgrund früherer Verschiebungen (siehe oben) sowie aufgrund des neuen Arbeitspakets zu Federated Learning (siehe unten) verschoben. Zusätzlich lagen die notwendigen Spezifikationen der Pilotanwendung von Orange erst gegen Ende der ursprünglichen Projektarbeit vor, was AP 4.3 weiter verzögert hat. Entsprechend wurde die Verlängerung des Projekts bis Ende 2024 beantragt und genehmigt, um die gemeinsamen Arbeiten mit unseren Projektpartnern INRIA und Orange abschließen zu können.

AP-Nr. / Titel	4.4 Integration von GDP, TEEs und MPC
Bearbeitungszeitraum	M28-M31
Gesamtumfang	5,5 Personenmonate (3 PM Postdoc, 2,5 PM Doktorand)
Ziele des Arbeitspaketes	
❖ technische Integration von GDP, TEEs und MPC ❖ Sicherheitsbeweise nach AP 4.2 ❖ Implementierung und Evaluierung von GDP/MPC-Integrationsmodellen ❖ Abwägung von Sicherheit und Leistungsfähigkeit von GDP/MPC-Modellen	

In AP 4.3 wurde bereits eine neue Integration von MPC mit LDP und GDP beschrieben. Entsprechend lag der Fokus von AP 4.4 im Gegensatz zur ursprünglichen Planung auf der Integration von MPC und Trusted Execution Environments (TEEs). Trusted Execution Environments, wie IntelSGX oder ARM TrustZone, sind abgeschlossene Bereiche auf einer CPU, sogenannte Enklaven, in denen vertrauliche Berechnungen durchgeführt werden können. Im Idealfall sind die Berechnungen und deren Ergebnisse auch für den Besitzer der Hardware nicht einsehbar. Im Bereich MPC können mithilfe von TEEs strukturierte Zufallszahlen in der Offlinephase gebildet werden. Dazu werden in der Enklave strukturierte Zufallszahlen erzeugt und ein Share mit dem öffentlichen Schlüssel einer Partei verschlüsselt. So kann jede Partei genau ihren Share entschlüsseln und später in einer MPC-Onlinephase verwenden.

TEEs sind im Vergleich mit kryptographischen Methoden, z. B. homomorpher Verschlüsselung, sehr effizient, gleichzeitig aber auch anfällig für Side-Channel-Attacken [Jan+17], [Fei+21], [Gha+23]. Um die hohe Effizienz von TEEs trotzdem in Anwendungen mit hohen Sicherheitsanforderungen nutzen zu können, wurden zusammen mit der Robert Bosch GmbH Setups mit mehreren gegenseitig unabhängigen TEEs getestet, die Sicherheitsgarantien liefern, auch wenn die Sicherheit eines TEEs gebrochen wird. Vielversprechende Ergebnisse zur Kombination von TEEs und MPC sind dabei in eine Bachelorarbeit bei der Robert Bosch GmbH und darauf aufbauend in die Abschlussarbeit von Georgios Solakis (Universität Stuttgart) [17] eingeflossen. Darüber hinaus hat Georgios Solakis auch die Generierung von Matrizentripeln (AP 3.1) und Tensortripeln (AP 3.2) untersucht. Aktuell wird im Rahmen einer Masterarbeit an der Universität Stuttgart die Generierung von polynomialen Tupeln (AP

3.3) mit TEEs erforscht.

Erwartungsgemäß zeigen alle bisherigen Evaluationsergebnisse einen erheblichen Effizienzvorteil von TEE-basierten Offlinephasen im Vergleich mit kryptographischen Protokollen. Abhängig von den weiteren Ergebnissen sollen diese auf einer Fachkonferenz eingereicht und präsentiert werden.

Da die Kombination von MPC und GDP abweichend von der Vorhabensbeschreibung im Rahmen von AP 4.3 behandelt wurde, reduzierte sich die Anzahl der Personenmonate für AP 4.4 auf 2 Personenmonate (1 PM Postdoc, 1 PM Doktorand).

AP-Nr. / Titel	4.5 Integration von HE und MPC
Bearbeitungszeitraum	M31-M34
Gesamtumfang	5,5 Personenmonate (2,5 PM Postdoc, 3 PM Doktorand)
Ziele des Arbeitspaketes	
❖ technische Integration von HE und MPC ❖ Sicherheitsbeweise nach AP 4.2 ❖ Implementierung und Evaluierung von HE/MPC-Integrationsmodellen ❖ Abwägung von Sicherheit und Leistungsfähigkeit von HE/MPC-Modellen	

In diesem Arbeitspaket war ursprünglich die Integration von MPC mit auf Torus-LWE-basierten FHE-Schemata geplant, die vom Projektpartner Zama ursprünglich entwickelt und weiter vorangetrieben werden. Dabei unterscheidet sich Torus-LWE strukturell von den häufiger in MPC-Protokollen eingesetzten Ring-LWE-Varianten wie [BGV12]. Leider ist eine intensive Kooperation mit Zama nicht zustande gekommen, sodass wir die Forschungsfrage nicht klären konnten.

Stattdessen wurde der Fokus in Arbeitspaket AP 4.5 auf die Weiterentwicklung Ring-LWE-basierter Methoden für klassische MPC-Protokolle wie [DPSZ12] gelegt. Dabei wurden sowohl für linear-homomorphe als auch für fully-homomorphe Ring-LWE-basierte Systeme neue Packmethoden entwickelt. Diese Packmethoden erlauben es, zahlreiche Tensoren in einem einzigen Chiffretext so zu codieren, dass eine einzige Operation auf dem Chiffretext (z. B. eine Multiplikation) eine Faltung aller verschlüsselten Tensoren erzeugt. Während wir diese Konstruktion in [5] explizit zur Optimierung von Tensorfaltungen verwenden, lässt sie sich aber auch auf zahlreiche andere in MPC verwendete korrelierte Zufallszahlen (wie Matrizenmultiplikation) ausdehnen, wenn viele gleichartige korrelierte Zufallszahlen generiert werden müssen.

Aufgrund des veränderten Fokus hat sich der Arbeitsaufwand an AP 4.5 auf 2,5 PM (2,5 PM Doktorand) verringert. Die frei gewordenen 3 Personenmonate wurden im neuen Arbeitspaket zu MPC und Federated Learning genutzt (siehe unten). Die Arbeit an AP 4.5 fand zeitlich im Rahmen der Arbeit an AP 3.2 statt.

AP-Nr. / Titel	5.1 Plattform-Design
Bearbeitungszeitraum	M2-M7, M23-M26
Gesamtumfang	10,0 Personenmonate
Ziele des Arbeitspaketes	
❖ Anforderungen an CRYPTECS zur Integration von MPC und seine Integration mit anderen	

PPC-Technologien werden definiert
- ❖ Sicherheits- und Leistungsanforderungen an MPC für die Einsatzfähigkeit in einer cloud-basierten Plattform werden erforscht

Erwartungsgemäß hat die Robert Bosch GmbH die MPC-basierte Cloud-Plattform Carbyne Stack zur Verfügung gestellt und während des Projektzeitraums stetig weiterentwickelt. Die Anforderungen von MPC an eine Cloud-Umgebung werden damit erfüllt (A.5.1.1). Im Rahmen von A.5.1.1 hat die Universität Stuttgart durch Beiträge auf der zugehörigen, jährlich stattfindenden Fachkonferenz CarbyneStackConf zur Entwicklung der Plattform beigetragen.

Mit der Festlegung auf Carbyne Stack und damit auf die zugrunde liegende MPC-Plattform [MP-SPDZ] mussten die in AP 3.1–AP 3.3 neu entwickelten MPC-Protokolle entsprechend ausgestaltet werden, sodass sie mit den bereits in MP-SPDZ vorhandenen MPC-Modulen kompatibel sind (AP 5.1.2), z. B. mit der Schlüsselgenerierung, der klassischen Beavertripelgenerierung oder bestehenden Onlineprotokollen. Die Arbeit mit MP-SPDZ hat sich dabei aufgrund der hohen Komplexität des Codes und der zu Projektbeginn noch fehlenden guten Dokumentation als Herausforderung herausgestellt. Wie in AP 3.1–AP 3.3 bereits beschrieben, konnten mittels MP-SPDZ jedoch sehr effiziente Implementierungen für unsere neuen Protokolle geschrieben werden, die neben unseren neu entwickelten effizienten Ansätzen auch die zahlreichen Optimierungen von MP-SPDZ nutzen und somit eine hohe Effizienz liefern.

AP-Nr. / Titel	6.1 Demonstration und Validierung
Bearbeitungszeitraum	M16-M17, M33-M36
Gesamtumfang	8,0 Personenmonate
Ziele des Arbeitspaketes	
❖ Analyseframework für Effizienz von MPC im Rahmen von Cloud-Anwendungen ❖ Integration der Forschungsergebnisse aus AP 3.1-4.5 werden in CRYPTECS implementiert ❖ Sicherheit der MPC-Module in CRYPTECS wird verifiziert	

Für die Analyse unserer MPC-Protokolle (AP 6.1.1) orientieren wir uns an in der Vergleichsliteratur genutzten Evaluationsmetriken. Insbesondere ermitteln wir die Laufzeit der Protokolle, die Menge an versendeten Daten und die Anzahl der Kommunikationsrunden pro Partei unter gewissen Rahmenbedingungen für die von uns optimierten Operationen Matrizenmultiplikation, Tensorfaltung und die Evaluation multivarianter Polynome (AP 6.1.2). Um ein möglichst genaues Bild der potenziellen Anwendungsmöglichkeiten zu zeichnen, wurden verschiedene Netzwerksetups betrachtet, d. h. verschiedene Bandbreitenbeschränkungen, lokale Rechnerleistungen und Netzwerkverzögerungen.

Die Evaluationsergebnisse (AP 6.1.3) sind in die jeweiligen Veröffentlichungen [4, 5, 12] eingegangen. Über die Selbstevaluation hinaus haben wir nicht nur unsere theoretischen Ergebnisse im Rahmen der Veröffentlichung begutachten lassen, sondern zusätzlich auch unsere Implementierung zur Begutachtung eingereicht. So wurden beispielsweise die Implementierungen zur Tensorfaltung [5] und polynomialen Tupeln [12] sowie zu [7] als Softwareartifacts der jeweiligen Konferenz akzeptiert [22, 23, 24]. Die Arbeiten an AP 6.1 fanden zeitlich zusammen bzw. kurz nach den Arbeiten an AP 3.1–AP 3.3 bzw. AP 4.3 (für die Integration von MPC und DP) statt.

AP-Nr. / Titel	7.1 Projektorientierter Ergebnistransfer
Bearbeitungszeitraum	M1-M36

Gesamtumfang	2,0 Personenmonate
Ziele des Arbeitspaketes	
❖ Bereitstellung von Software auf Open Source Plattformen ❖ kontinuierlicher Ausbau und Pflege der Vernetzung innerhalb der akademischen Community sowie der Industrie ❖ Öffentlichkeitsarbeit, etwa am Tag der Wissenschaft	

Die von uns im Projekt entwickelte Software ist komplett auf Open-Source-Plattformen verfügbar. Über den Projektzeitraum hinweg haben wir bei zahlreichen internationalen Topkonferenzen und als Gastdozenten unsere Ergebnisse präsentiert, z. B. bei IEEE Symposium on Security and Privacy 2022 in San Francisco (USA), ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2023) in Melbourne (Australien), Privacy Enhancing Technologies Symposium (PETS) 2023 in Lausanne (Schweiz), Privacy Enhancing Technologies Symposium (*PETS*) 2024 in Bristol (England), Asiacrypt 2024 in Kolkata (India), TPMPC 2023 in Aarhus (Dänemark), TPMPC 2024 in Darmstadt (Deutschland), Vortrag an der Royal Holloway University im Juni 2023 (England), CarbyneStackConf 2022 in Stuttgart (Deutschland), CarbyneStackConf 2023 und 2024 in Renningen (Deutschland) oder dem ACM Symposium on Eye Tracking Research & Applications (ETRA) 2024 in Glasgow (England).

2.2. Neue Arbeitspakete

Im Laufe des Projekts haben sich weitere über den ursprünglichen Forschungsantrag hinausgehende Fragestellungen mit Bezug zu CRYPTECS entwickelt. Wie bereits in den Zwischenberichten ausgeführt, haben wir in anderen Arbeitspaketen frei gewordene Personenmonate genutzt, um diese im Rahmen von CRYPTECS zu untersuchen. Wir möchten im Folgenden unsere zusätzlichen Forschungsergebnisse kurz beschreiben.

Strukturierte Zufallszahlen über Ringen der Charakteristik 2. Unsere Forschungsergebnisse in AP 3.1-3.3 zu neuen strukturierten Zufallszahlen erweitern die schnellsten aktiv-sicheren MPC-Protokolle [DSPZ12] und [KPR18] über einem Grundkörper mit Primcharakteristik. Beide Protokolle wurden in den letzten Jahren auf Grundringe $\mathbb{Z}/2^k$ erweitert.

Derartige Ringe sind besonders geeignet für die Implementierung mit Computern, da sie natürlich mit binären Daten arbeiten. Dieser Entwicklung folgend, erweitert unser Artikel unsere Ergebnisse in A.3.1 (und teilweise unsere Ergebnisse aus A.3.2 und A.3.3) von Kreisteilungsringen über einem endlichen Grundkörper zu Kreisteilungsringen über einem Ring $\mathbb{Z}/2^k$. Die Erweiterung von einem Grundkörper zu einem Ring ist dabei nicht offensichtlich, da es im Ring im Allgemeinen sehr viele nicht invertierbare Elemente bzw. Nullteiler gibt. Diese lassen sich von Angreifern nutzen, um die Sicherheit zu brechen. So kann ein Angreifer z. B. einen "selective failure"-Angriff starten, bei dem er seine Daten so verändert, dass sie mit einer gewissen (nicht zu hohen) Wahrscheinlichkeit zum Abbruch des Protokolls führen. Aus der Tatsache, ob das Protokoll tatsächlich abbricht oder nicht, lassen sich dann Rückschlüsse auf die von den anderen MPC-Parteien verwendeten Zufallszahlen ziehen. Es gibt grundlegende Ergebnisse, die es unmöglich machen, in $\mathbb{Z}/2^k$ diesen Informationsverlust zu unterbinden. In unserer Arbeit umgehen wir dieses Problem erstmals, indem wir nur den Teil der Zufallszahlen weiterverwenden, der von dem Angriff nicht betroffen ist. Mit diesem Ansatz erhalten wir ein MPC-Protokoll, das um einen Faktor 2,2 schneller ist als die besten theoretischen Vorarbeiten (über Grundringe) und gegenüber den besten existierenden ringbasierten Implementierungen sogar einen Faktor 10,2 schneller ist.

Unser Artikel wurde auf der Top-Konferenz "Privacy Enhancing Technologies Symposium" 2024 präsentiert und ist als [7] in den Proceedings erschienen. Zusätzlich wurde die Implementierung [23] getrennt begutachtet und als Softwareartifact zu PETS 2024 angenommen. Weiterhin wurden unsere Ergebnisse auch für die MPC-Top-Konferenz TPMPC 2024 als [9] angenommen und dort präsentiert.

Federated Learning und MPC. Das Arbeitspaket 4 der Teilvorhabensbeschreibung dient der Integration verschiedener PP-Technologien (privacy preserving technologies). Neben den im Antrag bereits beschriebenen Technologien MPC, DP, FHE, wurde Federated Learning (FL) neu als eine weitere PP-Technologie identifiziert, die im Rahmen der CRYPTECS-Anwendungsfälle vielversprechend ist.
Federated Learning ermöglicht das gemeinsame maschinelle Lernen (ML), wobei einzelne Klienten lokal eigene Modelle trainieren und diese immer wieder zu einem gemeinsamen Modell kombinieren. Dabei müssen nicht länger die geheimen Trainingsdaten (z. B. Bilder von Personen, Personaldaten, Kommunikationsdaten) zwischen den Klienten ausgetauscht werden, sondern nur noch das lokal erstellte ML-Modell. Dieses Modell hängt immer noch von den geheimen Eingangsdaten ab und muss daher geschützt werden. Da ein großer Teil des Rechenaufwandes, d. h. das lokale Training, aber von den einzelnen Klienten übernommen wird, werden die PP-Berechnungen auf den lokalen Modellen einfacher. Dies erlaubt es, bisher als teuer betrachtete PP-Technologien wie MPC oder FHE einzusetzen, ohne dabei Abstriche bei den Sicherheitsgarantien machen zu müssen. Zusätzlich scheinen FL-basierte Lösungen auch von den Projektpartnern (wie der Robert Bosch GmbH) und im Rahmen der im Projektverlauf bereits etablierten Softwarelösungen (wie Carbyne Stack [Car21]) umsetzbar.

Entsprechend wurde als Erweiterung der bisherigen APs 4.2–4.5 zusätzlich die Integration von MPC mit Federated Learning untersucht. Mit unserem Artikel „Federated Learning for Appearance-based Gaze Estimation in the Wild“ [10] im NeuRIPS 2022 Workshop on Gaze Meets ML (https://arxiv.org/abs/2211.07330) liefern wir einen ersten Schritt zur Untersuchung der Privatheitsgarantien von FL im Rahmen einer Anwendung im Bereich des maschinellen Lernens. In „PrivatEyes: Appearance-based Gaze Estimation Using Federated Secure Multi-Party Computation“ [11] zeigen wir, dass die Sicherheitsgarantien MPC-unterstützten Federated Learnings erheblich besser sind als bei reinen Federated-Learning-Lösungen. Hierbei wird die Kombination/Aggregation der oben beschriebenen lokalen Modelle vollständig in MPC durchgeführt. Dazu tauschen die Klienten ihre lokalen Modelle nicht länger direkt aus (bzw. nutzen nicht länger einen zentralen, mehr oder minder vertrauenswürdigen Server zur Aggregation), sondern verteilen jedes der lokalen Modelle (informationstheoretisch sicher) auf verschiedene Server. Diese Server übernehmen dann die Aggregation in einem aktiv sicheren MPC-Protokoll.

Unser Artikel wurde auf der Top-Konferenz „International Conference on Human-Computer Interaction“ (HCI 2024) präsentiert und ist als [11] in den Proceedings erschienen.
Aufbauend auf diesen Arbeiten bereiten wir zurzeit mehrere Artikel vor, die die Datensicherheit im Bereich Eye Tracking und Federated Learning weiter erhöhen. So liefert [15] das erste datensichere Protokoll zur Analyse der Bildqualität, die im FL-Training genutzt wird; [16] ermöglicht es, persönliche Präferenzen beim Datenschutz automatisch zu erkennen und entsprechend geeignete kryptographische Schutzmaßnahmen einzusetzen. Beide Artikel sind bei der Top-Konferenz „Privacy Enhancing Technologies Symposium“ 2026 zur Begutachtung eingereicht.

Weitere veröffentlichte Forschungsergebnisse. Die beiden Paper [3] und [6] betrachten den Effekt von Replay-Attacken, einer grundlegenden Angriffsmethode gegen Aggregationsprotokolle. Hierbei vervielfältigt ein Angreifer den verschlüsselten Input einer ehrlichen Partei. Zwar kann der Angreifer den Inhalt des Chiffretextes nicht direkt einsehen, er kann jedoch die Kopien in PP-Berechnungen einbringen und damit den Effekt des einzelnen Inputs auf ein später veröffentlichtes Ergebnis übersteigern. Somit kann der Angreifer aus dem Ergebnis statistisch auf den Inhalt des Inputs schließen. Mögliche Anwendungen im Rahmen von CRYPTECS betreffen Federated Learning.

Die Arbeit [2] liefert eine Anwendung automatisierter Zero-Knowledge (ZK) Beweissysteme, sogenannter SNARKs, und zeigt deren Potenzial für große (z. B. industrielle) Anwendungen. ZKPs (zurzeit noch nicht automatisierter Art) werden klassisch in der Offlinephase unserer MPC-Protokolle verwendet.

In [1] behandeln wir höhere Sicherheitsgarantien in MPC. Unsere MPC-Protokolle in 3.1–3.3 liefern bereits ein sehr hohes Sicherheitslevel: Die sensiblen Daten ehrlicher Parteien bleiben stets geheim, und jedes ausgegebene Ergebnis ist richtig, selbst wenn die Mehrheit der Parteien aktiv versucht, die Berechnung zu stören oder Daten abzugreifen. Dem Angreifer bleibt jedoch die Möglichkeit, einen Abbruch der Berechnung zu erzwingen, und dies, ohne dass ehrliche Parteien den Angreifer identifizieren und zukünftig ausschließen können. Hier setzt [1] an und liefert „Robustheit“, d. h.,

ehrliche Parteien können trotz einer gewissen Anzahl unehrlicher Parteien die Berechnung noch erfolgreich abschließen. Weiterhin ermöglicht [1] auch, Angreifer zu identifizieren und somit haftbar zu machen.

Fazit. Die in der Teilvorhabensbeschreibung formulierten Forschungsziele wurden größtenteils erreicht und teilweise übertroffen. Die Veröffentlichung noch ausstehender Ergebnisse, wie zu Fixpunkten und zur Kombination von MPC und Differential Privacy, ist in Vorbereitung. Über den Antrag hinausgehend wurden weitere, für die Integration von MPC in industrielle Anwendungen relevante Forschungsergebnisse erzielt. Das CRYPTECS-Verbundprojekt und insbesondere das Teilprojekt der Universität Stuttgart liefert damit sicheres MPC-basiertes maschinelles Lernen, das zukünftig von Industrieunternehmen genutzt werden kann und schon jetzt bei unseren Industriepartnern im Einsatz ist.

3. Wichtigste Positionen des zahlenmäßigen Nachweises

Position	Abgerechnete Ausgaben in €	Finanzierungsplan in €
0812 Beschäftigte E12-E15	505.586,87	472.198,67
0822 Beschäftigungsentgelte	4.319,49	25.968,60
0846 Dienstreisen	6.803,03	29.760,00

4. Verwertungsplan

4.1. Wirtschaftliche Erfolgsaussichten

MPC-basierende Technologien gewinnen zunehmend das Interesse industrieller Anwender. Dies hat mehrere Gründe. Zum einen sind Unternehmen durch gesetzliche Regelungen dazu gezwungen, strengen Datenschutzrichtlinien einzuhalten. Insbesondere hat die Europäische Union mit der Datenschutz-Grundverordnung (DSGVO) Maßstäbe in Punkto Datenschutz und Schutz der Privatsphäre ihrer Bürger gesetzt, die in ähnlicher Form auch mehr und mehr Einzug in Verordnungen von Ländern außerhalb der EU finden. Zum anderen wird der Wert von Daten auch über IT-Giganten hinaus erkannt, insbesondere im Kontext sehr datenintensiver ML-Anwendungen. Die in diesem Projekt entwickelten PPC-Technologien helfen, das Spannungsfeld zwischen Datenschutz und Nutzung von Daten aufzulösen. Dabei werden durch die erreichten Effizienzsteigerungen, z. B. aufgrund der deutlich effizientere MPC-Protokolle für ML-Anwendungen oder durch unsere systematische Integration mehrerer PPC-Technologien, neue Anwendungskontexte erschlossen, welche von Anwendungen im Gesundheitswesen über das Autonome Fahren und das Benchmarking von Unternehmen bis hin zur datensicheren Halbleiterproduktion reichen. Die Bedeutung von Maschinellem Lernen und künstlicher Intelligenz ist für derartige Anwendungen (und im Allgemeinen) im Vergleich zum Projektbeginn 2021 im Projektzeitraum noch einmal erheblich gestiegen und dominiert derzeit die industrielle Entwicklung weltweit.

Neben unserem Hauptanwendungsfeld maschinelles Lernen zeigen unsere Pilotanwendungen aus AP 4.3, dass unsere neuen MPC-Lösungen und integrierten Systeme auch über ML hinaus relevante Anwendungen haben, die im Fall von AP 4.3 bereits bei unserem Kooperationspartner Orange genutzt werden.

Grundsätzlich lassen sich die Ergebnisse von CRYPTECS überall dort anwenden, wo Berechnungen auf sensiblen Daten von mehreren Parteien durchgeführt werden müssen. Die Carbyne Stack-Plattform bietet dabei erstmals eine cloudbasierte MPC-Lösung, die ohne größere kryptographische Vorkenntnisse unmittelbar von Unternehmen eingesetzt werden kann. Carbyne Stack wird in der

Zwischenzeit von zahlreichen führenden deutschen Unternehmen wie SAP getestet und in deren eigenes Angebot integriert. Wir gehen davon aus, dass sich diese Entwicklung in den nächsten Jahren fortsetzt und zunehmend mehr Unternehmen mit Carbyne Stack auf datensichere, cloudbasierte Berechnungen zurückgreifen. Mit der Einbindung der Open-Source-Software MP-SPDZ, in die unsere Forschungsergebnisse aus diesem Projekt unmittelbar eingeflossen sind, kann und wird Carbyne Stack gleichzeitig auch zukünftig automatisch die neuesten Forschungsergebnisse aus akademischer Forschung nutzen können.

Zudem werden die Ergebnisse von CRYPTECS auch für unsere eigene Forschung weiterhin eine wichtige Rolle spielen. Insbesondere werden wir diese nutzen, um damit weitere Anwendungs- und Forschungsfelder zu erschließen, sowohl mit Partnern innerhalb der Universität Stuttgart als auch mit externen akademischen und industriellen Partnern. Unsere ersten auf CRYPTECS aufbauenden Arbeiten sind [19, 20, 21].

4.2. Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Unsere Arbeiten an MPC-Protokollen beschreiben eine Forschungsrichtung, in der systematisch zentrale Operationen für Anwendungsklassen direkt von MPC-Protokollen besonders effizient unterstützt werden. Bisher hat sich die Forschung mehr auf generische MPC-Lösungen konzentriert, die entsprechend nicht so effizient sind wie die in diesem Projekt verfolgten Ansätze. Mit Matrizenoperationen, Tensorfaltungen und Aktivierungsfunktionen wurden in diesem Projekt die MPC-Berechnungen für wesentliche Bestandteile von ML-Architekturen verbessert. Wir erwarten, dass unsere Arbeit in den nächsten Jahren fortgesetzt wird und weitere MPC-Operationen – auch außerhalb von ML-Anwendungen – nach unserem Vorbild optimiert werden.

Die Forschung im Bereich von PPC-Technologien hatte sich bis Projektstart vor allem auf einzelne Technologien konzentriert. In diesem Projekt haben wir gezeigt, dass (nicht triviale) Kombinationen von PPC-Technologien, wie in AP 4.2, Vorteile gegenüber Standardlösungen in realen Anwendungsfällen wie unserer Pilotanwendung haben. Auch hier gehen wir davon aus, dass sowohl unsere konkreten neuen Lösungen als auch der grundsätzliche Ansatz, PPC-Technologien zu kombinieren, über das Projekt hinaus von der wissenschaftlichen Community weiterverfolgt werden.

Daneben ist und wird die Forschung im Rahmen dieses Projektes auch unmittelbar in die Lehre der Universität Stuttgart, insbesondere des Instituts für Informationssicherheit, eingehen. Bereits während des Projekts hat sich eine Abschlussarbeit [17] und ein studentisches Forschungsprojekt [18] mit Fragestellungen der Vorhabensbeschreibung beschäftigt. Darüber hinaus betreuen wir zurzeit eine weitere Masterarbeit im Grenzbereich zwischen TEEs und MPC. Neben Abschlussarbeiten werden unsere Ergebnisse auch in unseren Vorlesungen, Praktika und Seminaren präsentiert.

Alle in diesem Teilprojekt erzielten Ergebnisse wurden oder sollen noch auf führenden internationalen Tagungen und in internationalen Top-Zeitschriften veröffentlicht werden, sodass auch andere Wissenschaftlerinnen und Wissenschaftler die hier begonnene Forschung weiterführen können.

5. Erfolgte und geplante Veröffentlichungen

5.1 Peer-Review Konferenzen and Veröffentlichungen in Fachzeitschriften

[1] Marc Rivinius, Pascal Reisert, Daniel Rausch, and Ralf Küsters: *Publicly Accountable Robust Multi-Party Computation*. In 2022 IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, US, May 22-26, pp. 2430-2449. Siehe auch https://eprint.iacr.org/2022/436.

[2] Nicolas Huber, Ralf Küsters, Toomas Krips, Julian Liedtke, Johannes Müller, Daniel Rausch, Pascal Reisert, and Andreas Vogt: *Kryvos: Publicly Tally-Hiding Verifiable E-Voting*. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, pp. 1443-1457. Siehe auch https://eprint.iacr.org/2022/1132.

[3] David Mestel, Johannes Müller, and Pascal Reisert: *How Efficient are Replay Attacks against Vote Privacy? A Formal Quantitative Analysis*. In 35th IEEE Computer Security Foundations Symposium, CSF 2022, Haifa, Israel, August 7-10, pp. 179-194. Siehe auch https://eprint.iacr.org/2022/743.

[4] Pascal Reisert, Marc Rivinius, Toomas Krips, and Ralf Küsters: *Overdrive LowGear 2.0: Reduced-Bandwidth MPC without Sacrifice*. In Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security, ASIACCS 2023, Melbourne, Australia, July 10-14, pp. 372-386. Siehe auch https://eprint.iacr.org/2023/462.

[5] Marc Rivinius, Pascal Reisert, Sebastian Hasler, and Ralf Küsters: *Convolutions in Overdrive: Maliciously Secure Convolutions for MPC*. In Proceedings on Privacy Enhancing Technologies 2023(3) / 23rd Privacy Enhancing Technologies Symposium, PoPETs/PETS 2023, Lausanne, Switzerland and Online, July 10-15, pp. 321-353. Siehe auch https://eprint.iacr.org/2023/359.

[6] David Mestel, Johannes Müller, and Pascal Reisert: *How Efficient are Replay Attacks against Vote Privacy? A Formal Quantitative Analysis (Extended Version)*. Journal of Computer Security, Volume 31, Issue 5, 2023

[7] Sebastian Hasler, Pascal Reisert, Marc Rivinius and Ralf Küsters: *Multipars: Reduced-Communication MPC over Z2k*. In Proceedings on Privacy Enhancing Technologies, Bristol, United Kingdom, July 15-20, 2024. Siehe auch https://eprint.iacr.org/2023/1932.

[8] Marc Rivinius, Pascal Reisert, Toomas Krips, Sebastian Hasler and Ralf Küsters: *Optimizing Preprocessing for Maliciously Secure MPC: Faster Matrix Multiplications and Convolutions without Sacrifice.* In Theory and Practice of Multi-Party Computation Workshop (TPMPC'24), Darmstadt, Germany, June 3-6.

[9] Sebastian Hasler, Pascal Reisert, Marc Rivinius and Ralf Küsters: *Multipars: Reduced-Communication MPC over Z2k*. In Theory and Practice of Multi-Party Computation Workshop (TPMPC'24), Darmstadt, Germany, June 3-6.

[10] Mayar Elfares, Zhiming Hu, Pascal Reisert, Andreas Bulling, and Ralf Küsters: *Federated Learning for Appearance-based Gaze Estimation in the Wild*. In Proceedings of the 1st NeurIPS Gaze Meets ML Workshop / Proceedings of Machine Learning Research (Volume 210), GMML/PMLR 2022, New Orleans, LA, USA, December 3, pp. 20-36.

[11] Mayar Elfares, Pascal Reisert, Zhiming Hu, Wenwu Tang, Ralf Küsters, and Andreas Bulling. 2024. PrivatEyes: Appearance-based Gaze Estimation Using Federated Secure Multi-Party Computation. Proc. ACM Hum.-Comput. Interact. 8, ETRA, Article 232 (May 2024), 23 pages. Siehe auch https://arxiv.org/abs/2402.18970.

[12] Pascal Reisert, Marc Rivinius, Toomas Krips, Sebastian Hasler and Ralf Küsters: *Actively Secure Polynomial Evaluation from Shared Polynomial Encodings*. In International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2024), Kolkota, India, December 9-13, 2024. Siehe auch Technical Report [13] und https://eprint.iacr.org/2024/1435.

5.2 Preprints und Technische Berichte

[13] Pascal Reisert, Marc Rivinius, Toomas Krips, and Ralf Kuesters: *Arithmetic Tuples for MPC*. In Cryptology ePrint Archive, Paper 2022/667.

[14] Ferran Escobar, Andreas Athanasiou, Ralf Küsters, Pascal Reisert: *Optimizing Differential Privacy in Federated Analytics under Known Input Distributions*. Submitted to IEEE Computer Security Foundations Symposium 2026.

[15] Mayar Elfares, Pascal Reisert, Ralf Küsters, and Andreas Bulling: *QualitEye: Public and Privacy-preserving Gaze Data Quality Verification*. ArXiv e-prints, Art. no. arXiv:2506.05908, 2025.

doi:10.48550/arXiv.2506.05908. Submitted to Privacy Enhancing Technologies Symposium, PoPETs/PETS 2026.

[16] Mayar Elfares, Pascal Reisert, Ralf Küsters, and Andreas Bulling: *Gaze3P: Gaze-Based Prediction of Perceived Privacy*. Submitted to Privacy Enhancing Technologies Symposium, PoPETs/PETS 2026.

[17] Georgios Solakis: *Distributed Generation of Correlated Randomness with Trusted Execution Environments.* Abschlussarbeit am Institut für Informationssicherheit der Universität Stuttgart. Betreuer: Pascal Reisert und Ralf Küsters, 2024.

[18] Carmen Wabartha: *Fixpunktoperationen in gitterbasierten Mehrparteien-Protokollen.* Forschungsprojekt am Institut für Informationssicherheit der Universität Stuttgart. Betreuer: Pascal Reisert und Ralf Küsters, 2024.

5.3 Unsere auf CRYPTECS aufbauenden Projekte und Arbeiten (ab 2025)

[19] Marc Rivinius, “MPC with Publicly Identifiable Abort from Pseudorandomness and Homomorphic Encryption,” in *Advances in Cryptology - EUROCRYPT 2025*, S. Fehr and P.-A. Fouque (Eds.), Springer, 2025, pp. 270–300.

[20] Mayar Elfares, Salma Younis, Pascal Reisert, Ralf Küsters, Tobias Renner, Andreas Bulling: *Guidelines for Gaze-based Neural Preliminary Diagnosis.* ArXiv preprint arXiv:2506.08517, 2025. doi:10.48550/arXiv.2506.08517.

[21] Sebastian Hasler, Pascal Reisert, and Ralf Küsters: *Pseudorandom Correlation Functions from Ring-LWR*. Submitted to the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2025)

5.4 Peer-Review Softwareartifacts

[22] Marc Rivinius, Pascal Reisert, Sebastian Hasler, and Ralf Küsters: *Convolutions in Overdrive: Maliciously Secure Convolutions for MPC*. In Proceedings on Privacy Enhancing Technologies 2023(3) / 23rd Privacy Enhancing Technologies Symposium, PoPETs/PETS 2023, Lausanne, Switzerland and Online, July 10-15, pp. 321-353. Artifact: https://petsymposium.org/popets/2023/popets-2023-0084.php

[23] Sebastian Hasler, Pascal Reisert, Marc Rivinius and Ralf Küsters: *Multipars: Reduced-Communication MPC over Z2k*. In Proceedings on Privacy Enhancing Technologies, Bristol, United Kingdom, July 15-20, 2024. Artifact: https://petsymposium.org/popets/2024/popets-2024-0038.php

[24] Pascal Reisert, Marc Rivinius, Toomas Krips, Sebastian Hasler and Ralf Küsters: *Actively Secure Polynomial Evaluation from Shared Polynomial Encodings*. In International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2024), Kolkota, India, December 9-13, 2024. Artifact: https://artifacts.iacr.org/asiacrypt/2024/a4/

6. Weitere Literaturangaben

[ABL+18] David W. Archer, Dan Bogdanov, Yehuda Lindell, Liina Kamm, Kurt Nielsen, Jakob Illeborg Pagter, Nigel P. Smart, Rebecca N. Wright, “From Keys to Databases—Real-World Applications of Secure Multi-Party Computation”. *Computer Journal* 61(12), pp. 1749-1771, 2018.

[All19] Joshua Allen et al. “An algorithmic framework for differentially private data analysis on trusted processors”. In *Neural Information Processing Systems*, pp. 13635-13646, 2019.

[Bea92] Donald Beaver, “Efficient Multiparty Protocols Using Circuit Randomization”. In *Advances in Cryptology* (CRYPTO ’91), pp. 420-432, 1992.

[BGV12] Zvika Brakerski, Craig Gentry, Vinod Vaikuntanathan, “(Leveled) Fully Homomorphic Encryption Without Bootstrapping”. In ITCS ’12, pp. 309–325, 2012.

[Car21] Carbyne Stack Contributors. 2021. Carbyne Stack: Open Source Cloud Native Secure Multiparty Computation. Verfügbar unter https://carbynestack.io

[CKR+20] Hao Chen, Miran Kim, Ilya Razenshteyn, Dragos Rotaru, Yongsoo Song, Sameer Wagh, “Maliciously Secure Matrix Multiplication with Applications to Private Deep Learning”. In *Advances in Cryptology* (ASIACRYPT 2020), pp. 31-59, 2020.

[DPSZ12] Ivan Damgård, Valerio Pastro, Nigel P. Smart, Sarah Zakarias, “Multiparty Computation from Somewhat Homomorphic Encryption”. In CRYPTO 2012, pp. 643-662, 2012.

[Fei+21] Shufan Fei, Zheng Yan, Wenxiu Ding, and Haomeng Xie. Security vulnerabilities of sgx and countermeasures: A survey. CSUR , 2021.

[Gha+23] Moein Ghaniyoun, Kristin Barber, Yuan Xiao, Yinqian Zhang, and Radu Teodorescu. Teesec: Pre-silicon vulnerability discovery for trusted execution environments. ISCA , 2023.

[HBA24] R. Hernandez, O. G. Bautista and K. Akkaya, "Optimizing the Parameters of Pipelined Multi-Party Computation for Privacy-Preserving Machine Learning Applications," *IEEE ICC 2024*, 2024, pp. 938-943, doi: 10.1109/ICC51166.2024.10623002.

[Hua+24] Zhicong Huang, Wen-jie Lu, Yuchen Wang, Cheng Hong, Tao Wei, and WenGuang Chen. 2024. Coral: Maliciously Secure Computation Framework for Packed and Mixed Circuits. In ACM CCS '24. ACM, New York, NY, USA, 810–824.

[Jan+17] Yeongjin Jang, Jaehyuk Lee, Sangho Lee, and Taesoo Kim. Sgx-bomb: Locking down the processor via rowhammer attack. SysTEX , 2017.

[KOV15] Peter Kairouz, Sewoong Oh, Pramod Viswanath, “Secure Multi-party Differential Privacy”. In *Advances in Neural Information Processing Systems* (NIPS 2015), pp. 2008-2016, 2015.

[KPR18] Marcel Keller, Valerio Pastro, Dragos Rotaru, “Overdrive: Making SPDZ Great Again”. In *Advances in Cryptology* (EUROCRYPT 2018) pp. 158-189, 2018.

[LW24] Liang, Z., Wang, H. FedST: secure federated shapelet transformation for time series classification. *The VLDB Journal* **33**, 1617–1641 (2024). https://doi.org/10.1007/s00778-024-00865-w

[MNPS04] Dahlia Malkhi, Noam Nisan, Benny Pinkas, Yaron Sella, “Fairplay-Secure Two-Party Computation System”. In *USENIX Security Symposium*, pp. 287-302, 2004

[MZ17] Payman Mohassel, Yupeng Zhang, “SecureML: A System for Scalable Privacy-Preserving Machine Learning”. In *IEEE Symposium on Security and Privacy* (S&P 2017), pp. 19-38, 2017.

[MP-SPDZ] N1 Analytics. MP-SPDZ. https://github.com/data61/MP-SPDZ. 2021.

[WHZ24] Wu, W., Homsi, S., Zhang, Y. (2024). Confidential and Verifiable Machine Learning Delegations on the Cloud. In ESORICS 2024, Springer, Cham.

[Yao86] Andrew Chi-Chih Yao, “How to generate and exchange secrets”. In *IEEE Symposium on Foundations of Computer Science*, pp. 162-167, 1986.