

Sachbericht zum Verwendungsnachweis

Kurzbericht (Teil I)

ZE: Robert Bosch GmbH	Förderkennzeichen: 16KIS1440K
Vorhabenbezeichnung: Cloud-Ready Privacy-Preserving Technologies - CRYPTTECS -; Entwicklung einer Cloud Plattform für das Privacy-Preserving Computing	
Laufzeit des Vorhabens: 01.07.2021 – 30.09.2024	
Berichtszeitraum: 01.07.2021 – 30.09.2024	

1. Motivation

Der Schutz der Privatsphäre und die Befähigung der Menschen zum souveränen Umgang mit ihren persönlichen Daten sind entscheidende Voraussetzungen für die Stärkung des Vertrauens in die digitale, datenbasierte Wirtschaft. Studien zeigen, dass die Bürgerinnen und Bürger erhebliche Bedenken in Bezug auf Cybersicherheit und Datenschutz haben. Diese Bedenken müssen ausgeräumt werden, damit die Menschen neue Technologien annehmen, insbesondere im Schlüsselbereich der Künstlichen Intelligenz. Europäische Unternehmen haben die Chance, nachhaltiges Kundenvertrauen in datenschutzfreundliche Produkte und Dienstleistungen aufzubauen und langfristig erhebliche Marktanteile zu gewinnen, indem sie die Bedürfnisse sicherheits- und datenschutzbewusster Kunden erfüllen. Vertrauen ist auch eine Voraussetzung für den Austausch von Daten innerhalb der Wirtschaft. Technische Datenschutzmechanismen können eine wichtige Rolle bei der Bewältigung dieser Herausforderungen spielen. Gegenwärtig mangelt es solchen Technologien jedoch noch an Reife, was einer breiten industriellen Nutzung entgegensteht.

2. Zielsetzung

Das CRYPTTECS-Projekt zielte darauf ab, eine Cloud-Plattform für Privacy-Preserving Computing zu entwickeln, um die industrielle Anwendung entsprechender Technologien zu ermöglichen. Die Plattform sollte verschiedene Techniken wie Secure Multiparty Computation (MPC), Homomorphic Encryption (HE) und Differential Privacy in Form von wiederverwendbaren Cloud-Diensten integrieren. Eine Herausforderung bestand darin, diese Techniken zu verbessern und, wo sinnvoll, kombinierbar zu machen, um sichere und effiziente Dienste für maschinelles Lernen und Datenanalyse zu ermöglichen. Die Integration mit nativen Cloud-Technologien war ein zentrales Ziel, um einen Einsatz im Unternehmenskontext zu ermöglichen. CRYPTTECS sollte durch die Bereitstellung einer dedizierten Plattform für den Schutz der Privatsphäre die Zusammenarbeit zwischen Unternehmen erleichtern und das Vertrauen der Kunden in den Umgang mit ihren Daten stärken. Die Validierung der Technologie erfolgte bei Bosch anhand einer Anwendung im Bereich des länderübergreifenden Datenaustauschs im Personalwesen auf Konzernebene.

3. Ablauf des Vorhabens und wesentliche Ergebnisse

Die Robert Bosch GmbH koordinierte den deutschen Teil des CRYPTTECS-Konsortiums und stellte die technische Infrastruktur für die Zusammenarbeit bereit.

Im Rahmen der Anforderungserhebung wurden seitens Bosch zwei Pilotanwendungsfälle, "People Analytics" (unternehmensübergreifende Auswertung von Personaldaten) und

"Battery-in-the-Cloud" (Batterieüberwachung und Optimierung der Lebensdauer für batterieelektrische Fahrzeuge in der Cloud), identifiziert, analysiert und die Anforderungen an die CRYPT ECS-Plattform dokumentiert.

Der Fokus der PPC-technikspezifischen Verbesserungen lag auf der Kostenoptimierung von MPC-Offline-Verfahren. In Kooperation mit der Universität Stuttgart wurden Fortschritte im Bereich von *Pseudo Random Correlation Generators* (PCGs) auf algorithmischer Ebene und bei den Implementierungstechniken erzielt. Der Ansatz wird in einer Kooperation mit der University of Technology Sydney, mit dem Ziel Hardwarebeschleunigung zur weiteren Effizienzsteigerung einzusetzen, weiter vorangetrieben. Zusätzlich wurde von Bosch ein alternativer Ansatz auf Basis von Confidential Computing (CC) entwickelt und als Proof-of-Concept implementiert. Dieser wird in einer Kooperation mit dem Center of Data for Public Good des Indian Institute of Science weiterentwickelt.

Bei der Plattformentwicklung diente die von Bosch entwickelte Carbyne Stack Plattform als Basis für die MPC-Funktionalität und wurde im Projektverlauf in vielerlei Hinsicht verbessert und erweitert. Ein Microservice für die MPC-Offlinephase wurde entworfen und implementiert. Er unterstützt die Integration verschiedener Methoden zur Erzeugung von korreliertem Zufallsmaterial (PCG-basiert, CC-basiert, HE-basiert), die ein breites Spektrum von Leistungs-, Kosten- und Sicherheitsanforderungen abdecken. Zusätzlich wurde eine Authentifizierungs- und Autorisierungsschicht implementiert und Deployment-Mechanismen für verschiedene Cloud-Umgebungen bereitgestellt. Ein Proof-of-Concept für den kombinierten Einsatz von CC und MPC ("Defense in Depth") wurde gemeinsam mit dem Konsortialpartner Edgeless Systems erstellt.

Bezüglich der anwendungsnahen Dienste wurde ein Serverless Computing Ausführungsmodell für MPC implementiert und die Machbarkeit von MPC-basierter Inferenz auf Bilddaten demonstriert. Ein Machine-Learning-as-a-Service Proof-of-Concept mit CC-basiertem Ende-zu-Ende-Schutz von personenbezogenen Daten wurde umgesetzt. Die Entwicklung eines Data Analytics Dienstes erfolgte in Zusammenarbeit mit der Boston University. Da die Integration in die Plattform nicht fristgerecht abgeschlossen werden konnte, hat Bosch einen maßgeschneiderten alternativen Ansatz zur Durchführung der Validierung des „People Analytics“ Use Case umgesetzt. Für den Anwendungsfall „Battery-in-the-Cloud“ wurde eine Architektur für Federated Learning mit sicherer Aggregation mittels MPC und Schutz der ML-Modelle durch CC entworfen und als Open-Source-Prototyp veröffentlicht.

Im Rahmen der Demonstration und Validierung wurden Evaluationskriterien für den Anwendungsfall "People Analytics" definiert und die Performance der MPC-basierten Lösung in einem realitätsnahen Cloud-Setup experimentell validiert. Ein externes und durch Zweitmeinungen abgesichertes Rechtsgutachten bestätigte die Eignung von MPC zur Anonymisierung personenbezogener Daten unter bestimmten Voraussetzungen im Allgemeinen und für den Einsatz im Kontext des „People Analytics“ Use Case zur Reduktion von Compliance-Kosten bei der unternehmensübergreifenden Datenverarbeitung im Speziellen.

Das Open-Source-Projekt Carbyne Stack wurde von Bosch Ende 2021 ins Leben gerufen. Jährlich stattfindende Konferenzen („CarbyneStackCon“) und Vorträge auf Fachkonferenzen dienen der Öffentlichkeitsarbeit und der Verbreitung der Projektergebnisse. Bosch erhielt für die Arbeit am Carbyne Stack 2022 den Deutschen IT-Sicherheitspreis. Im Rahmen des Open-Source-Projektes, das Anfang 2025 zur Linux Foundation Europe übertragen werden soll, arbeitet Bosch mit einer wachsenden Anzahl von internationalen Partnern zusammen, zu denen unter anderem SAP und Resolve zählen. Resolve gehört zur WPP Group, der weltweit größten Werbeholding.

Sachbericht zum Verwendungsnachweis

Ausführlicher Bericht (Teil II)

ZE: Robert Bosch GmbH	Förderkennzeichen: 16KIS1440K
Vorhabenbezeichnung: Cloud-Ready Privacy-Preserving Technologies – CRYPTTECS: Entwicklung einer Cloud Plattform für das Privacy-Preserving Computing	
Laufzeit des Vorhabens: 01.07.2021 – 30.09.2024	
Berichtszeitraum: 01.07.2021 – 30.09.2024	
Datum 31.03.2025	

Inhalt

1. Aufzählung der wichtigsten wissenschaftlich-technischen Ergebnisse und anderer wesentlicher Ereignisse	3
1.1. Gesamtarbeitspaket 1 (Projektkoordination und -management)	3
1.1.1 Arbeitspaket 1.1 (Verbundkoordination und Projektmanagement)	3
1.2. Gesamtarbeitspaket 2 (Anforderungserhebung und Technische Analyse).....	3
1.2.1 Arbeitspaket 2.1 (Definition und Auswahl der Pilotanwendungen)	3
1.2.2 Arbeitspaket 2.2 (Anforderungsanalyse)	4
1.3. Gesamtarbeitspaket 3 (PPC-Technik-spezifische Verbesserungen)	4
1.3.1 Arbeitspaket 3.1 (Effiziente MPC-Offlinephase)	4
1.4. Gesamtarbeitspaket 5 (Konzeptionierung und Umsetzung der Plattform)	6
1.4.1 Arbeitspaket 5.1 (Grundlegende CRYPTTECS Plattform)	6
1.4.2 Arbeitspaket 5.2: Umsetzung der anwendungsnahen PPC-Dienste.....	8
1.4.3 Arbeitspaket 5.3 (Experimentelle Evaluation).....	10
1.5. Gesamtarbeitspaket 6 (Demonstration und Validierung)	10
1.5.1 Arbeitspaket 6.1 (Definition von Evaluationskriterien für Pilotanwendungen) ...	11
1.5.2 Arbeitspaket 6.2 (Umsetzung der Pilotanwendungen).....	11
1.5.3 Arbeitspaket 6.3 (Validierung der Pilotanwendungen).....	11
1.6. Gesamtarbeitspaket 7 (Veröffentlichung, Verwertung und Standardisierung)	13
1.6.1 Arbeitspakete 7.1 (Stakeholder Vernetzung) und 7.2 (Community Aufbau und Pflege) 13	
2. Änderungen im Vergleich zur ursprünglichen Vorhabensbeschreibung.....	15
2.1. Fokus auf Kostenreduktion MPC / Privacy-Preserving Federated Learning	15
2.2. Wegfall Pilotanwendungsfall	16
2.3. Weitere Anpassungen	16
3. Fortschritte auf dem Gebiet des Vorhabens bei anderen Stellen.....	17
3.1. Effizientere Homomorphe Verschlüsselung	17
3.2. Kosteneffizientes MPC	17
3.3. Verbessertes Confidential Computing.....	17
3.4. Datenschutzfreundliches Federated Learning.....	18
4. Literaturverzeichnis	19

1. Aufzählung der wichtigsten wissenschaftlich-technischen Ergebnisse und anderer wesentlicher Ereignisse

Im Folgenden werden die im Berichtszeitraum durchgeführten Arbeiten und deren Ergebnisse nach Arbeitspaketen gegliedert dargestellt. Wo inhaltlich sinnvoll, werden Ergebnisse aus verschiedenen Arbeitspaketen zusammengefasst.

1.1. Gesamtarbeitspaket 1 (Projektkoordination und -management)

Im Rahmen dieses Arbeitspaketes hat die Robert Bosch GmbH die Koordination des deutschen Teils des CRYPTTECS-Konsortiums übernommen. Dies geschah in enger Abstimmung mit Orange S.A. als nationalem Koordinator auf französischer Seite.

1.1.1 Arbeitspaket 1.1 (Verbundkoordination und Projektmanagement)

Um eine effiziente und reibungslose Zusammenarbeit im CRYPTTECS-Konsortium zu ermöglichen, wurden einschlägige Kollaborationsplattformen evaluiert. Für den Aufbau der Infrastruktur für die Zusammenarbeit (D1.1.1) fiel die Wahl schließlich auf Google Workspace. Die dazugehörigen Arbeiten umfassten die Einrichtung und Pflege der Projektmailinglisten, die Bereitstellung der Infrastruktur für virtuelle Meetings und die Umsetzung einer Dokumentenablage mit Versionierung. Die Prozesse und Best Practices bezüglich der Themen Projektmanagement und Projektadministration, Kommunikation und Kooperation, Qualitätssicherungs- und Risikomanagement wurden in einem Projekthandbuch (D1.1.1) festgehalten. Der nach Projektantrag vorgesehene Integrationsworkshop (D1.1.2) entfiel, da ausschließlich Bosch Technologie in die Basisplattform integriert hat (siehe Abschnitt 1.4). Bosch war verantwortlich für die Organisation und Durchführung von monatlichen Status- und Planungstreffen auf Ebene des Gesamtkonsortiums sowie eines Präsenzworkshops zur Mitte der Projektlaufzeit.

1.2. Gesamtarbeitspaket 2 (Anforderungserhebung und Technische Analyse)

In diesem Arbeitspaket wurden für Bosch interessante Pilot-Anwendungsfälle identifiziert, analysiert und dokumentiert, die im weiteren Projektverlauf zur Validierung der Carbyne Stack Plattform herangezogen wurden. Bosch war auch für die Koordination der Aktivitäten in diesem Arbeitspaket zwischen den Projektpartnern verantwortlich.

1.2.1 Arbeitspaket 2.1 (Definition und Auswahl der Pilotanwendungen)

Ausgehend von den beiden ursprünglich von Bosch vorgeschlagenen und in der Gesamtvorhabenbeschreibung skizzierten Pilotanwendungsfällen wurde ein Katalog potenzieller Anwendungsfälle erstellt (D2.1.1). In den Erarbeitungsprozess wurden, wo sinnvoll, die Geschäftsbereiche der Robert Bosch GmbH und ihrer Tochtergesellschaften im Rahmen von Workshops eingebunden. Zwei Anwendungsfälle („People Analytics“ und „Battery-in-the-Cloud“) wurden ausgewählt und näher spezifiziert. Dabei wurden relevante Datenflüsse identifiziert und entsprechende Schutzziele definiert (D2.1.2). In einem nachgelagerten Schritt wurden die Pilotanwendungsfälle der Robert Bosch GmbH mit denen der Orange S.A. in einem Gesamtkatalog zusammengeführt (D2.1.3) und auf der CRYPTTECS-Webseite [1] (D2.2.1) veröffentlicht.

Veröffentlichungen

- Robert Bosch GmbH, Orange S.A.: *D2.1 Use Case Specification*. 2021. Abrufbar unter <https://www.cryptecs.eu/dissemination/deliverables>.

1.2.2 Arbeitspaket 2.2 (Anforderungsanalyse)

Für die ausgewählten Bosch-Pilotanwendungen „People Analytics“ und „Battery-in-the-Cloud“ sowie die Pilotanwendungen des Projektpartners Orange S.A. aus Arbeitspaket 2.1 (siehe Abschnitt 1.2.1) wurden die funktionalen und nicht-funktionalen Anforderungen an die CRYPTTECS-Plattform formal erfasst, katalogisiert, und dem Konsortium in Form eines konsolidierten Anforderungskatalogs zur internen Nutzung zur Verfügung gestellt (D2.2.1).

1.3. Gesamtarbeitspaket 3 (PPC-Technik-spezifische Verbesserungen)

Ziel dieses Arbeitspaketes war es, die Grenzen der einzelnen PPC-Verfahren, insbesondere MPC, HE, DP und TEEs, zu untersuchen und dort, wo es aus Sicht der Pilot-Anwendungsfälle notwendig war, Verbesserungen zu erarbeiten. Der Schwerpunkt der Arbeiten der Robert Bosch GmbH lag auf der Kostenoptimierung von MPC-Offline-Verfahren.

1.3.1 Arbeitspaket 3.1 (Effiziente MPC-Offlinephase)

Im Rahmen dieses Arbeitspaketes beschäftigte sich Bosch mit der Entwicklung von Verfahren zur Erzeugung von korreliertem Zufallsmaterial, das für den kosteneffizienten Einsatz von Secure Multiparty Computing mit aktiver Sicherheit von entscheidender Bedeutung ist, da bei Verwendung existierender kryptographischer Verfahren die Kosten der Offline-Phase die der Online-Phase um mindestens eine Größenordnung übersteigen. Insbesondere beim Einsatz in Cloud-Umgebungen, in denen der Netzwerkverkehr hohe Kosten verursachen kann, wirkt sich dies erheblich negativ auf die Wirtschaftlichkeit von MPC-basierten Lösungen aus.

Der Fokus der Arbeiten lag auf der Weiterentwicklung und der konkreten Implementierung von sogenannten „Pseudo Random Correlation Generators“ (PCGs). PCGs sind noch junge kryptographische Verfahren, die vor allem die Kommunikationskosten im Vergleich zu bestehenden Verfahren, die auf homomorpher Verschlüsselung oder Oblivious Transfer basieren, deutlich reduzieren. Obwohl signifikante Fortschritte bei der effizienten Implementierung von PCGs gemacht werden konnten, wurde die notwendige technische Reife für den geplanten Einsatz in der Basisplattform während der Projektlaufzeit leider nicht erreicht. Um das Problem der hohen Kommunikationskosten dennoch adressieren zu können, wurde an einer alternativen Implementierung einer kosteneffizienten Offline-Phase auf Basis von Confidential Computing (CC) Technologien gearbeitet.

1.3.1.1 Arbeitsschritt 3.1.1 (Algorithmische Verbesserungen von PCGs)

Dieses Arbeitspaket befasste sich mit der theoretischen Effizienzsteigerung von PCGs, insbesondere für die Erzeugung von authentifizierten Beaver-Triples für aktiv sichere Multiplikationen in MPC-Protokollen. Dazu wurde das zu diesem Zeitpunkt kommunikationseffizienteste Protokoll von Boyle et al. [2] analysiert und optimiert. Es konnten signifikante Verbesserungen in mehreren Bereichen erzielt werden: 7% in der Kommunikation, 20% in der Berechnung während der interaktiven Phase und 11% in der Menge des korrelierten Zufallsmaterials. Um diese Verbesserungen zu erreichen, wurde ein neuartiges, aktiv sicheres Protokoll erarbeitet, das die effiziente Erzeugung von authentifizierten, geheimen, gemeinsam genutzten skalierten Einheitsvektoren ermöglicht.

Diese Vektoren sind ein wesentlicher Baustein aktueller PCG-Protokolle und dienen als Grundlage für die effiziente Erzeugung authentifizierter Beaver-Tripel.

Veröffentlichungen

- Rieder, V. (2025). *Generation of Authenticated Secret-Shared Scaled Unit Vectors for Beaver Triples*. In: Eichlseder, M., Gambs, S. (eds) Selected Areas in Cryptography – SAC 2024. SAC 2024. Lecture Notes in Computer Science, vol 15516. Springer, Cham. https://doi.org/10.1007/978-3-031-82852-2_3

Patentanmeldungen

- Vincent Rieder, Christoph Bösch, Sven Trieflinger: *COMPUTERIMPLEMENTIERTES VERFAHREN UND VORRICHTUNG ZUR VERTEILTEN ERZEUGUNG KORRELIERTER PSEUDOZUFÄLLIGKEIT* (DE 102024209652.0)

1.3.1.2 Arbeitsschritt 3.1.2 (Effiziente Implementierung von PCGs)

Auf Grundlage einer systematischen Analyse des PCG-Protokolls von Boyle et al. hinsichtlich verschiedener Kostenmetriken wurde eine effiziente Implementierung der theoretischen Ergebnisse aus Arbeitsschritt 3.1.1 realisiert. Hierfür kamen innovative Parallelisierungsstrategien und implementierungsfreundliche Dekompositionsansätze in einem modularen Gesamtkonzept zum Einsatz. Die daraus resultierende prototypische Implementierung *Silentium* stellt die erste vollständige Implementierung einer PCG-basierten Offline-Phase zur Erzeugung von Beaver-Tripeln dar.

Zusätzlich zu den bereits erwähnten Optimierungen der Kommunikationskosten von PCGs um etwa drei Größenordnungen, weist *Silentium* eine Laufzeitverbesserung von bis zu 33% im Vergleich zu alternativen Implementierungen zur Erzeugung von Beaver-Tripeln in der MPC-Bibliothek MP-SPDZ [3] auf, die aktuell den Stand der Technik repräsentiert.

Ein signifikanter Anteil des Rechenaufwands bei PCG-Verfahren entsteht durch die Auswertung von „Number Theoretic Transforms“ (NTT) auf hochdimensionalen Polynomringen. Verbesserungen in diesem Bereich haben daher ein hohes Kostensenkungspotenzial. Um weitere Fortschritte in diesem Bereich zu ermöglichen, wurden Synergien genutzt, die sich aus einer Kooperation mit der University of Technology Sydney im Rahmen eines öffentlich geförderten Projekts in Australien ergaben. Dort wird an der Beschleunigung von NTTs durch die Auslagerung von Berechnungen auf verschiedene Hardwareplattformen (FPGAs, GPUs und hochoptimierte Befehlssätze auf CPUs) gearbeitet. Dadurch könnten perspektivisch weitere signifikante Einsparpotenziale realisiert werden. Die Kooperation wird nach Projektende im Rahmen des Carbyne Stack Open Source Projektes fortgesetzt.

Veröffentlichungen

- Vincent Rieder. *Silentium: Decomposition of a Pseudorandom Correlation Generator for Beaver Triples*. (in Vorbereitung)

Patentanmeldungen

- Vincent Sebastian Rieder, Enrico Sorbera, Sven Trieflinger, Christoph Bösch: *VORRICHTUNGEN UND VERFAHREN ZUR SICHEREN MEHRTEILNEHMERBERECHNUNG MIT KORRELIERTER ZUFÄLLIGKEIT* (DE 102023212693.1, US 18/970383, KR 10-2024-0185531)

1.3.1.3 Arbeitsschritt 3.1.3 (Integration in die CRYPTTECS-Plattform)

Trotz der oben beschriebenen Verbesserungen der PCGs auf algorithmischer und Implementierungsebene konnte die notwendige Reife zur Integration des Verfahrens in die CRYPTTECS-Basisplattform während der Laufzeit des Projektes nicht erreicht werden. Eine notwendige Verallgemeinerung der bekannten Verfahren zur Erzeugung von korreliertem Zufallsmaterial über Multiplikationstripel („Beaver Triple“) hinaus war aus zeitlichen Gründen leider nicht realisierbar. Aus dem gleichen Grund war auch eine Unterstützung von mehr als zwei MPC-Parteien nicht realisierbar. Dies sind interessante zukünftige Forschungsfelder.

Um dennoch das wichtige Anwendungshemmnis der hohen Kommunikationskosten in der Offline-Phase zu beseitigen, wurde ein alternatives Konzept auf Basis von Confidential Computing Technologien mit verschiedenen Realisierungsmöglichkeiten und unterschiedlichen Eigenschaften hinsichtlich Schutzniveau und Kostenersparnis entwickelt, zum Patent angemeldet und im Rahmen einer in Kooperation mit der Dualen Hochschule Baden-Württemberg betreuten Bachelorarbeit auf Basis von Open-Source-Komponenten in Form eines Proof-of-Concept implementiert und experimentell evaluiert. Die Ergebnisse wurden im Rahmen eines Vortrags auf dem Confidential Computing Mini Summit [4] einer breiteren Öffentlichkeit vorgestellt. Eine Integration der Implementierung in die CRYPTTECS-Basisplattform erfolgt derzeit in Zusammenarbeit mit dem Center of Data for Public Good (CDPG) in Indien im Rahmen des Carbyne Stack Open Source Projektes.

Veröffentlichungen

- Jonas Eppard: *Verwendung von Confidential Computing für sichere Mehrparteienberechnung*. Bachelorarbeit. Duale Hochschule Baden-Württemberg. 2023
- Sven Trieflinger: *PETs of the world unite! Conquer the middle ground in the performance vs security spectrum*. Contributed talk at Open Source Summit Europe 2023, Confidential Computing Mini Summit, Bilbao, Spain, September 19-21.

Patentanmeldungen

- Trieflinger Sven, Boesch Christoph, Rieder Vincent Sebastian, Eppard Jonas: *VERFAHREN ZUM BEREITSTELLEN VON KORRELIERTEN ZUFÄLLIGKEITEN FÜR EINE SICHERE MEHRPARTEIENBERECHNUNG* (DE 102023205012.9, US 18/662061, CN 202410678824.8)

1.4. Gesamtarbeitspaket 5 (Konzeptionierung und Umsetzung der Plattform)

Ziel des Arbeitspaketes war das Design und die Umsetzung der CRYPTTECS-Plattform gemäß den Anforderungen aus Gesamtarbeitspaket 2 (Anforderungserhebung und Technische Analyse) auf Basis der Ergebnisse aus Gesamtarbeitspaket 3 (PPC-Technik-spezifische Verbesserungen).

1.4.1 Arbeitspaket 5.1 (Grundlegende CRYPTTECS Plattform)

Nach Sichtung und Bewertung existierender Open-Source-Plattformen für das Privacy-Preserving Computing wurde als Basis für die MPC-basierte Funktionalität der CRYPTTECS-Plattform die bei Bosch vorentwickelte Plattform Carbyne Stack [5] ausgewählt. Design und Architektur des entsprechenden CRYPTTECS MPC-Subsystems wurden in einem Designdokument [6] dokumentiert (D5.1.1).

Die im Folgenden beschriebenen Arbeitsergebnisse wurden, sofern diese zur Veröffentlichung vorgesehen waren, über die Carbyne Stack GitHub Organisation [7] der Öffentlichkeit zur Verfügung gestellt.

Mit der Implementierung der MPC-Offlinephase im dafür entwickelten Carbyne Stack Microservice *Klyshko* [8] wurde die MPC-Basisfunktionalität (D5.1.2) der Plattform vervollständigt. Dabei wurden auch die Ziele der Arbeitsschritte 5.1.3 (Konzeption und Umsetzung von Mechanismen zur Erweiterung der Plattform) und 5.1.4 (Mechanismen für Multi-Cloud Koordination) berücksichtigt: Die modulare Kubernetes-native Architektur erlaubt die Integration beliebiger alternativer MPC-Offlinephasen über das abstrakte *Klyshko Integration Interface* (KII). Um diese Erweiterbarkeit zu demonstrieren, wurden zwei weitere Varianten zur Generierung von kryptographischem Material integriert: Neben der in Abschnitt 1.3.1.3 beschriebenen, auf Confidential Computing basierenden Variante wurde eine auf homomorpher Verschlüsselung basierende kryptographische Offline-Phase namens *Cowgear* aus dem MP-SPDZ Open Source Projekt integriert. Damit kann der Anwender aus einem Spektrum von drei Implementierungen mit unterschiedlichen Kosten und Sicherheitsgarantien, die für seine Anforderungen am besten geeignete auswählen. Die notwendige Koordination zwischen den Klyshko-Serviceinstanzen über Carbyne Stack Deployments hinweg erfolgt über den weitverbreiteten verteilten Key/Value-Speicherdienst *etcd*. *Klyshko* wurde auf der CarbyneStackCon 2023 [9] der Öffentlichkeit vorgestellt.

Für das halbautomatische Deployment der Plattform wurde in Arbeitspaket 5.1.5 ein *Infrastructure-as-Code*-Ansatz (IaC) über die Tools *Helm* und *Helmfile* im Carbyne Stack Software Development Kit (SDK) bereitgestellt. Später wurde diese Funktionalität um die Möglichkeit der lokalen Bereitstellung als Entwicklungsumgebung und in der Microsoft Azure Cloud als internetoffene oder internetisolierte Instanz erweitert (D5.1.1). Um einen möglichst hohen Automatisierungsgrad zu erreichen, wurde ein IaC-Ansatz auf Basis von *Hashicorp Terraform* verwendet. Dieser Ansatz lässt sich leicht auf andere Cloud-Plattformen übertragen, was der angestrebten Erweiterbarkeit (Arbeitsschritt 5.1.3) und der Anwendbarkeit über mehrere Clouds hinweg (Arbeitsschritt 5.1.4) zugutekommt. Eine Anleitung zum Deployment der Carbyne Stack Plattform inklusive einer Demonstrationsanwendung wurde in Form eines Tutorials auf der Carbyne Stack Webseite [5] veröffentlicht (D5.1.1). Damit wurden die Projektpartner in die Lage versetzt, Carbyne Stack Systeme auf eigener oder Public Cloud Infrastruktur bereitzustellen. Der Ansatz wurde bei der CarbyneStackCon 2023 [9] öffentlich vorgestellt.

In Zusammenarbeit mit dem Konsortialpartner Edgeless Systems wurde ein Proof-of-Concept zur Demonstration einer „Defense-in-Depth“-Strategie durch die Kombination von Confidential Computing und Computing on Encrypted Data Technologien in einem Stacking-Ansatz erstellt. Dabei wurde gezeigt, dass Carbyne Stack unverändert in einem Constellation Confidential Computing Kubernetes Cluster eingesetzt werden kann. Das Ergebnis ist eine mehrschichtige Sicherheitsarchitektur, die das Gesamtsystem auf Ebene der jeweiligen lokalen Infrastruktur der MPC-Parteien gegen böswillige Systemadministratoren und potenzielle Angreifer schützt. Der Ansatz wurde in einem Blogbeitrag [10] sowie in Vorträgen auf dem Confidential Computing Mini Summit 2023 [4] und einem Cloud Native Community Meetup in Bochum [11] vorgestellt.

Veröffentlichungen

- Robert Bosch GmbH: *Carbyne Stack GitHub Organization*. Verfügbar unter <https://github.com/carbynestack>.
- Robert Bosch GmbH: *WP5 PPC Platform Design and Realization*. 2022. Verfügbar unter <https://www.cryptecs.eu/dissemination/deliverables>.

- Jared Weinfurter: *Deploying Carbyne Stack using Infrastructure as Code*. Contributed talk at CarbyneStackCon 2023, Renningen, Germany.
- Sven Trieflinger: *Kubernetes-native Correlated Randomness Generation with Klyshko*. Contributed talk at CarbyneStackCon 2023, Renningen, Germany.
- Sven Trieflinger: *Defense in Depth for cloud-native Computing on Encrypted Data - Stacking Confidential Computing and Secure Multiparty Computation*, Carbyne Stack Medium Blog, October 15, 2023
- Sven Trieflinger: *PETs of the world unite! Conquer the middle ground in the performance vs security spectrum*. Contributed talk at Open Source Summit Europe 2023, Confidential Computing Mini Summit, Bilbao, Spain, September 19-21.
- Sven Trieflinger: *Carbyne Stack – Towards cloud-native enterprise-grade open MPC*, Contributed talk at Cloud Native Community Ruhr December Meetup, Bochum, Germany, December 5.

[1.4.1.1 Arbeitsschritt 5.1.6 \(Konzeption und Umsetzung einer Authentifizierungsschicht für Carbyne Stack\) und Arbeitsschritt 5.1.7 \(Konzeption und Umsetzung einer Berechtigungsschicht für Carbyne Stack\)](#)

Mit der Einführung des neuen Dienstes *Thymus* wurde die Sicherheitsarchitektur der Carbyne Stack Plattform um Authentifizierungsmaßnahmen erweitert. Die implementierten Authentifizierungsmechanismen wurden an die spezifischen Anforderungen der verschiedenen Kommunikationsschnittstellen innerhalb der Plattform angepasst: Die Authentifizierung für die Kommunikation zwischen den Diensten verschiedener Carbyne-Stack-Deployments erfolgt zertifikatsbasiert über Mutual TLS. Dies konnte durch die Nutzung der Funktionalität des Istio Service Mesh effizient umgesetzt werden. Für die Client-/Benutzer-seitige Authentifizierung wurden die cloud-nativen Open-Source Implementierungen Ory Kratos und Ory Hydra integriert. Ory Kratos verwaltet Benutzeridentitäten und Anmeldedaten, während Ory Hydra die Protokolle OAuth2 und OpenID Connect für die Generierung und Verifizierung von Authentifizierungstokens implementiert.

Aufbauend auf der Authentifizierungsfunktionalität wurde eine Autorisierungsschicht entworfen und implementiert. Dazu wurde die Open Source Autorisierungskomponente *Open Policy Agent* (OPA) in Thymus integriert und die relevanten Speicher- und Verarbeitungsdienste Amphora bzw. Ephemeral um eine flexible Autorisierungslogik erweitert.

Die bereitgestellten Authentifizierungs- und Autorisierungsfunktionen helfen dabei die komplexen Sicherheitsanforderungen im Unternehmenskontext zu erfüllen.

Veröffentlichungen

- Sven Trieflinger, Sebastian Becker, Benjamin Hettwer: *Thymus: Adding essential Security Features to the Carbyne Stack platform the Cloud-Native Way*. Contributed talk at CarbyneStackCon 2024, Renningen, Germany, November 27-28.

[1.4.2 Arbeitspaket 5.2: Umsetzung der anwendungsnahen PPC-Dienste](#)

Ziel dieses Arbeitspaketes war die Bereitstellung der für die Umsetzung der Pilotanwendungen erforderlichen anwendungsnahen PPC-Dienste.

1.4.2.1 Arbeitsschritt 5.2.1 (Umsetzung ausgewählter Programmier- und Ausführungsmodelle)

Auf der Ebene der Programmier- und Ausführungsmodelle wurde das Serverless Computing Ausführungsmodells mit Secure Multiparty Computation (MPC) Methoden (D5.2.1) kombiniert. Dabei kamen cloud-native Technologien, insbesondere der Container Orchestrator *Kubernetes*, das Service Mesh *Istio*, und das Serverless Computing Framework *Knative* zum Einsatz. Die Implementierung steht als *Ephemeral* [12] Microservice in der Carbyne Stack Plattform zur Verfügung.

1.4.2.2 Arbeitsschritt 5.2.2 (MLaaS Inferenz Dienst) und 5.2.3 (MLaaS Training Dienst)

Auf Basis des in Abschnitt 1.4.2.1 beschriebenen Ephemeral Serverless Computing Dienstes konnte die Machbarkeit von MPC-basierter Inferenz (D5.2.2) auf Basis eines neuronalen Netzes durch die Portierung eines existierenden Demonstrators zur Erkennung von handschriftlichen Ziffern (MNIST Datensatz) gezeigt werden. Ein Demonstrationsvideo steht auf der Carbyne Stack Webseite [5] zur Verfügung.

Neben den Arbeiten zur MPC-basierten Inferenz wurde ein Machine-Learning-as-a-Service (MLaaS) Proof-of-Concept mit Ende-zu-Ende Schutz von personenbezogenen Daten in AI-Pipelines unter Verwendung des *MarbleRun* Service Mesh des Konsortialpartners Edgeless Systems umgesetzt. Dabei wurden sowohl die mittels Trusted Execution Environments (TEE) abgesicherte Inferenz (D5.2.2) über eine Integration mit dem *KServe* Serverless Computing Framework (D5.2.1) und *TensorFlow* unter Verwendung des LibraryOS *Gramine*, als auch TEE-geschütztes Training (D5.2.3) eines neuronalen Netzes mittels Integration mit dem *KubeFlow* Machine Learning Framework umgesetzt. Die Zusammenarbeit mit Edgeless Systems erfolgte über das Bosch Venture Client Programm Open Bosch. Beim jährlich verliehenen Open Bosch Award wurde die Kooperation als eine der 10 besten Kooperationen nominiert. Technisch basieren Carbyne Stack und der PoC auf denselben Technologien, so dass eine Integration der Ansätze bei Bedarf unkompliziert umsetzbar wäre. Design und Implementierung des PoC wurden in einem Bericht dokumentiert und innerhalb des Konsortiums zur internen Verwendung zur Verfügung gestellt.

Die Inferenz auf Basis von FHE war nach Erkenntnissen des Konsortialpartners Orange S.A. während der Projektlaufzeit aufgrund des immensen Overheads nach dem Stand der Technik nicht realistisch und wurde daher nicht weiterverfolgt.

1.4.2.3 Arbeitsschritt 5.2.4 (Data Analytics Dienst)

Um eine Umsetzung des People Analytics Use Cases zu ermöglichen, wurde seitens Bosch eine Kooperation mit dem Rafik B. Hariri Institute for Computing and Computational Science & Engineering der Boston University aufgesetzt. Ziel der Kooperation war die Integration des MPC-basierten Secrecy Datenbankmanagementsystems [13] in Carbyne Stack und damit in die CRYPTTECS-Plattform (D5.2.5). Das Secrecy System wurde durch die Boston University modularisiert, sodass wesentliche Aspekte der angestrebten Integration in die Carbyne Stack Plattform, wie beispielsweise Dateneingabe und Datenausgabe oder die Bereitstellung des kryptographischen Materials, abgebildet werden konnten. Dazu wurde analog zum Klyshko-Dienst gemeinsam mit Partnern aus der Carbyne Stack Open Source Community ein Erweiterungskonzept für den Rechendienst Ephemeral erarbeitet (vgl. Arbeitsschritt 5.1.3). Die Integration selbst konnte während der Laufzeit des Projektes nicht fertiggestellt werden. Stattdessen wurde bei Bosch eine alternative Lösung erarbeitet, um die Anforderungen aus dem Anwendungsfall „People Analytics“ erfüllen zu können (siehe Abschnitt 1.5.2).

1.4.2.4 Arbeitsschritt 5.2.5 (Federated Learning)

Um den ursprünglich vorgesehenen „Battery-in-the-Cloud“ Anwendungsfall zu unterstützen, wurde eine Architektur erarbeitet, die Federated Learning mit Secure Aggregation über MPC auf Basis von Carbyne Stack ermöglicht. Neben der sicheren Aggregation über MPC wurde auch ein Konzept erarbeitet, das Confidential Computing Techniken zum Schutz potenziell sensibler oder wertvoller ML-Modelle während des Trainings auf Clientseite einsetzt. Die Idee wurde prototypisch umgesetzt [14], zum Patent angemeldet und auf dem Flower Summit 2023 der Öffentlichkeit vorgestellt [15]. Während der ursprünglich geplante Use Case „Battery-in-the-Cloud“ nicht weiterverfolgt werden konnte, könnten die Arbeitsergebnisse zukünftig im Bereich der rechtskonformen grenzüberschreitenden Datennutzung bei Bosch eine Rolle spielen.

Veröffentlichungen

- Sven Trieflinger: *Nettle - Privacy-Preserving FL based on Flower and Carbyne Stack*. Contributed talk at Flower Summit 2023, Cambridge, United Kingdom, May 30-31.

Patentanmeldungen

- Zimmermann Christian, Trieflinger Sven, Becker Sebastian, Weinfurter Jared: *VERTRAULICHES VERTEILTES MASCHINELLES LERNEN* (DE 102023204816.7, US 18/660573, CN 202410649544.4)

1.4.3 Arbeitspaket 5.3 (Experimentelle Evaluation)

Ziel des Arbeitspaketes war die Bereitstellung von Infrastruktur für die kontinuierliche Erhebung von Evaluationsdaten zu den nicht-funktionalen Eigenschaften der CRYPTTECS Plattform und ihrer Dienste.

1.4.3.1 Arbeitsschritte 5.3.1 (Definition von Metriken) und 5.3.2 (Automatisiertes Analyseframework)

In einem vorbereitenden Schritt wurden zu erfassende Metriken auf Ebene der Dienste der Carbyne Stack Plattform ausgewählt. Zur kontinuierlichen Leistungsbewertung (D5.3.1) der Carbyne Stack Plattform wurde anschließend das *Caliper-System* auf Basis des bestehenden *Load-Testing-as-Code* Frameworks *Gatling* konzipiert und umgesetzt. Konzept und Implementierung wurden in einem Vortrag auf der Carbyne Stack Conference 2023 der Öffentlichkeit vorgestellt [16].

Veröffentlichungen

- Julian Grewe: *Continuous Load Testing using Caliper*. Contributed talk at CarbyneStackCon 2023, Renningen, Germany, November 30.

1.4.3.2 Arbeitsschritt 5.3.3 (Analyse von Ressourcennutzung und Kosten)

Die Analyse der Ressourcennutzung und die Ableitung der damit verbundenen Kosten fand direkt in den ausgewählten relevanten Arbeitspaketen 3.1 (Effiziente MPC-Offlinephase) und Arbeitspaket 6.2 (Umsetzung der Pilotanwendungen) statt.

1.5. Gesamtarbeitspaket 6 (Demonstration und Validierung)

Das Ziel dieses Arbeitspaketes bestand in der Selektion und Dokumentation der technischen, rechtlichen, geschäftlichen sowie organisatorischen Bewertungskriterien für die Bosch Pilotanwendungen. Auf Basis dieser Bewertungskriterien sollte eine Validierung der Pilotanwendungen erfolgen.

Tabelle 1 zeigt beispielhaft die Ergebnisse der experimentellen Performance-Analyse der Online-Phasen in einem realitätsnahen WAN-Setup zwischen MPC-Parteien, die in Azure- und AWS-Rechenzentren im Großraum Frankfurt gehostet wurden, für einfache SELECT-Abfragen und eine komplexere Age-Distribution-Abfrage, die eine aufwändige Sortierung der Datenreihen erfordert, in Kombination mit Protokollen für verschiedene Sicherheitsmodelle [3]. Die Auswirkungen der bekannten EDABITS-Optimierung zur Reduzierung des Datentransfervolumens auf die verschiedenen Protokolle werden ebenfalls dargestellt. Der für die Analyse verwendete Datensatz umfasste mehr als 411.000 Datenreihen.

Attribute		SELECT, incl. SUM, COUNT, AVG				Age distribution incl. SORT			
		MASCOT	SPDZ2K	Semi	Semi2k	MASCOT	SPDZ2K	Semi	Semi2k
w/o edaBits	Time (WAN) [s]	698.47	600.69	372.64	382.66	7650.28	8253.3	3062.16	2841.2
	Rounds	531,345	531,347	329,283	329,283	4,109,887	5,638,755	2,063,107	2,063,107
	Global data sent [MB]	1727.4	1701.06	1699.08	418.19	111,538	111,553	45,602	22,774
w/ edaBits	Time (WAN) [s]	955.05	842.94	533.89	481.59	8262.29	8901.49	3544.87	3119.37
	Rounds	654,829	654,831	370,443	370,443	4,168,703	5,697,571	2,121,913	2,121,913
	Global data sent [MB]	84.87	84.67	55.40	35.40	107,801	107,868	41,868	20,951

Tabelle 1: Ergebnisse der experimentellen Analyse für beispielhafte SQL-Abfragen in einem Setup mit über ein Wide-Area-Netzwerk verbundenen, auf Azure und AWS gehosteten MPC-Parteien

Die Kosten der Offline-Phase wurden in der Analyse nicht berücksichtigt, da sie bei Verwendung des Correlated Randomness Generators auf Basis von Confidential Computing (vgl. Abschnitt 1.3.1) vernachlässigbar sind. Folgende Aussagen können getroffen werden:

- Die Laufzeitunterschiede zwischen den Protokollen (max. Faktor ~3) sind deutlich geringer als zwischen den Abfragetypen (max. Faktor ~10). Dies ist vor allem auf die aufwändige Sortierung der Datenbankeinträge zurückzuführen, die bei der Abfrage nach der Altersverteilung erforderlich ist.
- Die Unterschiede in der übertragenen Datenmenge zwischen den Protokollen (bis zu einer Größenordnung) und zwischen den Abfragetypen (bis zu zwei Größenordnungen) sind beträchtlich.
- Die durch den Einsatz von EDABITS erzielbaren Einsparungen beim Datenvolumen sind für einfache SELECT-Abfragen signifikant, führen aber gleichzeitig zu einer Erhöhung der Rechenzeit. Bei den komplexeren Abfragen sind die Einsparungen beim Datentransfer dagegen vernachlässigbar.
- Die Kosten pro Abfrage der Age-Distribution, die sich aus den Kosten für die virtuellen Maschinen und den Kosten für den ausgehenden Netzwerkverkehr zusammensetzen, sind sehr unterschiedlich und liegen zwischen ca. 2 € bei Verwendung des Semi2k-Protokolls und über 10 € bei Verwendung des SPDZ2K-Protokolls. Für einfache SELECT-Anfragen liegen die Kosten deutlich unter einem Euro pro Abfrage.

Zusammenfassend zeigt die experimentelle Analyse, dass der Einsatz von MPC für die datenschutzfreundliche Analyse von Personaldaten, die typischerweise einmal monatlich im Batch-Betrieb erfolgt, durchaus praktikabel ist. Unter der Annahme, dass die MPC-Parteien nicht böswillig handeln, kann der Einsatz von Protokollen für das „Honest-but-Curious“-Setting (z.B. Semi2k) erhebliche Einsparpotenziale bieten.

Gemäß einem externen Rechtsgutachten, das von zwei weiteren unabhängigen Experten bestätigt wurde, ist MPC ein robustes Instrument zur Anonymisierung von Daten, sofern bestimmte Kriterien eingehalten werden. Zu den wichtigsten Aspekten gehört, dass die

MPC-Parteien von unabhängigen juristischen Personen betrieben werden und dass die Abfrageergebnisse keine personenbezogenen Informationen oder personenbeziehbaren Informationen enthalten.

Bosch prüft eine mögliche Anwendung der Arbeitsergebnisse in verschiedenen internen Data Lake Anwendungsszenarien.

Veröffentlichungen

- Sebastian Becker, Christoph Bösch, Benjamin Hettwer, Thomas Hoeren, Merlin Rombach, Sven Trieflinger, Hossein Yalame: *Multi-Party Computation in Corporate Data Processing: Legal and Technical Insights*. Cryptology ePrint Archive. Paper 2025/463. <https://eprint.iacr.org/2025/463>

1.6. Gesamtarbeitspaket 7 (Veröffentlichung, Verwertung und Standardisierung)

Das Ziel dieses Gesamtarbeitspaketes war es, Stakeholder einzubinden und eine externe Community aufzubauen, um Feedback zu erhalten und Beiträge Dritter zu stimulieren.

1.6.1 Arbeitspakete 7.1 (Stakeholder Vernetzung) und 7.2 (Community Aufbau und Pflege)

1.6.1.1 Arbeitsschritt 7.1.1 (Ermittlung und Einbindung von Stakeholdern) und Arbeitsschritt 7.2.1 (Aufbau Open Source Infrastruktur und Community)

Im September 2021 hat die Robert Bosch GmbH das Open-Source-Projekt *Carbyne Stack* [7] mit der initialen Kontribution einer intern entwickelten Codebasis (D7.2.1) ins Leben gerufen. Diese Codebasis bildet die technische Grundlage für die CRYPTTECS-Basisplattform. Um die notwendige Rechtssicherheit bei der Veröffentlichung der Codebasis zu gewährleisten, waren umfangreiche rechtliche Prüfungen und die Umsetzung von Compliance Maßnahmen notwendig (z.B. rechtskonforme Docker Basisimages, Software Bills of Materials, exportkontrollrechtliche Deklarationen, *Developer Certificate of Origin* als rechtssicherer und fairer Kontributionsmechanismus). Diese Maßnahmen ermöglichen eine risikoarme Nutzung der Open-Source-Software durch Dritte, insbesondere während der Projektlaufzeit durch die Partner im CRYPTTECS-Konsortium.

Flankiert wurde die initiale Kontribution durch Maßnahmen zur Etablierung einer Community rund um das Open-Source Projekt, wie zum Beispiel die Organisation öffentlicher virtueller Community-Meetings oder die Bereitstellung von Dokumentation für Kontributoren und Maintainer. Zudem wurde eine zugehörige Webseite (D7.2.1) [5] entwickelt und kontinuierlich gepflegt (D7.2.2). Zur Unterstützung der Öffentlichkeitsarbeit ist die Robert Bosch GmbH Ende 2021 der MPC Alliance, einem Interessenverband zur Förderung der MPC-Technologie, beigetreten (D7.1.1).

Die Veröffentlichung von Carbyne Stack als Open-Source Projekt ist auf durchweg positive Resonanz in Industrie und Forschung gestoßen, wie folgende beispielhafte Rückmeldungen belegen:

- “*Great initiative/work [...]! Keep on pushing forward.*”
(Dr. Markus Hablitzel, Innovation Manager, Munich Re)
- “*That's great! We will try that right at the next opportunity!*”
(Dr. Axel Schröpfer, PETS, SAP Research)

- *“Congrats. Real transformational leadership demonstrated.”*
(Richard Curran, Security Officer Datacenter Group, Intel)
- *“This is really cool!!”*
(Vikas Bathia, Head of Product for Azure Confidential Computing)

In den darauffolgenden Jahren konnte die Open Source Community um Carbyne Stack kontinuierlich um weitere Partner aus aller Welt erweitert werden (D7.2.3). Honda (Japan), die University of Technology Sydney (Australien), SAP (Deutschland), Cybernetica (Estland), das Center of Data for Public Good (CDPG, Indien) und zuletzt Resolve (Dänemark) sind seither aktiv in die Weiterentwicklung der Carbyne Stack Plattform eingebunden. Ein wichtiger Meilenstein war dabei insbesondere der Einstieg von SAP in das Open-Source Projekt [17]. Gemeinsam wurde an einer sprachagnostischen Client-Software für Carbyne Stack gearbeitet, die technisch auf Web Assembly basiert. Darauf aufbauend entstand die Idee für ein Browser-Plugin, das die niedrigschwellige Verwendung von MPC-Diensten über den Browser ermöglichen soll.

In den Jahren seit 2022 organisierte die Robert Bosch GmbH mit der CarbyneStackCon [18] [9] [19] jährlich eine zweitägige öffentliche Community-Konferenz mit Vorträgen und Workshops rund um das Thema Secure Multiparty Computation im Kontext des Carbyne Stack Open-Source Projektes. Neben Teilnehmern aus dem Kreis des CRYPTTECS-Konsortiums, fanden jeweils über 60 weitere Teilnehmer aus über 30 Organisationen ihren Weg zum Veranstaltungsort in Stuttgart (2022) bzw. Renningen (2023f). Rennommierte Experten aus den Bereichen Datenschutz und Secure Multiparty Computation hielten Vorträge und trugen zu einem gelungenen Wissensaustausch bei. Mitarbeiter von Bosch leisteten mit zahlreichen Vorträgen wertvolle Beiträge zum Erfolg der Konferenzreihe.

Um den Bekanntheitsgrad in Wissenschaft und Wirtschaft zu erhöhen, wurden Vorträge auf einschlägigen Technologie- und Industriekonferenzen gehalten. Dazu zählen Beiträge auf der StackConf 2022 [20], TPMPC 2022 [21], dem Flower Summit 2023 [15] und dem Open Source Summit North America [22].

Ein weiterer Schwerpunkt der Öffentlichkeitsarbeit lag auf der Nutzung von LinkedIn. Mit über 30 Beiträgen wurden über 150.000 Impressionen generiert und über 1600 Reaktionen ausgelöst. Darüber hinaus wurde ein Medium Blog [23] initiiert, der bislang 4 Artikel zu verschiedenen Themen rund um Carbyne Stack umfasst.

Im Jahr 2022 haben sich die Initiatoren des Carbyne Stack Projektes für den 9. Deutschen IT-Sicherheitspreis [24] beworben und sich erfolgreich gegen ein hochkarätiges Bewerberfeld aus der deutschen IT-Sicherheitsforschung durchgesetzt. Das Preisgeld von 20.000 Euro für den 3. Platz kam gleichermaßen der Weiterentwicklung des Carbyne Stack als auch der Öffentlichkeitsarbeit, insbesondere der Ausrichtung der CarbyneStackCon 2023, zugute.

Für das Frühjahr 2025 ist die Übergabe des Projekts an die Linux Foundation Europe geplant. Damit werden die Voraussetzungen für das weitere Wachstum der Carbyne Stack Plattform auf neutralem Boden geschaffen. Bereits jetzt haben verschiedene Parteien angekündigt, Carbyne Stack in den Produktiveinsatz bringen zu wollen.

2. Änderungen im Vergleich zur ursprünglichen Vorhabensbeschreibung

Im Folgenden werden die mit dem Projektträger abgestimmten aufkommensneutralen Änderungen des Arbeitsprogramms gegenüber der ursprünglichen Vorhabensbeschreibung dargestellt.

2.1. Fokus auf Kostenreduktion MPC / Privacy-Preserving Federated Learning

Bosch sieht in MPC eine zentrale Privacy-Preserving-Computing-Technologie, die auch über das CRYPTTECS-Projekt hinaus von großer Bedeutung sein wird. Die Kostenreduktion spielt dabei eine zentrale Rolle, um die Technologie für den kommerziellen Einsatz fit zu machen. Bosch hat daher in enger Zusammenarbeit mit der Universität Stuttgart und weiteren Partnern im Rahmen des Gesamtarbeitspakets 3 (PPC-Technologie-spezifische Verbesserungen) in die Verbesserung und Umsetzung der Ergebnisse der Arbeiten zum Thema „Silent MPC“ (vgl. Abschnitt 1.3.1) investiert. Im Gegenzug wurden die Arbeitsschritte 5.1.3 zur Konzeption und Umsetzung von Mechanismen zur Erweiterung der Plattform und 5.3.2 zum automatisierten Analyseframework im Umfang deutlich reduziert und in andere Arbeitspakete integriert.

Die Techniken des Confidential Computing haben während der Projektlaufzeit einen hohen Reifegrad erreicht, der weitere Forschungs- und Entwicklungsarbeiten an den Basistechnologien bei Bosch überflüssig machte. Die Kombination von Confidential Computing mit Secure Multiparty Computing erschien jedoch weiterhin vielversprechend und spielte daher im weiteren Arbeitsprogramm, insbesondere in den Arbeitspaketen 5.1.2 (Integration von PPC-Basisdiensten und Bereitstellung von Hilfsdiensten) und 5.3.5 (Federated Learning) eine wichtige Rolle. Die Bedeutung von Federated Learning hat sowohl in der Wissenschaft als auch für Unternehmen erheblich an Relevanz gewonnen. Die Robert Bosch GmbH hat dem durch eine Anpassung des Arbeitsprogramms in Abstimmung mit dem Projektträger Rechnung getragen.

Im Einzelnen wurden folgende Änderungen vorgenommen:

- Ergänzung des Arbeitspaketes 3.1 in Gesamtarbeitspaket 3 (PPC-Technik-spezifische Verbesserungen) mit dem Schwerpunkt *Pseudorandom Correlation Generators* (PCGs) zur Senkung der Kosten für MPC (**insgesamt +12 PM**) mit den Unterarbeitspaketen:
 - AP 3.1.1 Algorithmische Verbesserungen für PCG-Schemata (4 PM)
 - AP 3.1.2 Effiziente Implementierung von PCGs (6 PM)
 - AP 3.1.3 Integration in die CRYPTTECS-Plattform (2 PM)
- Ergänzung des Arbeitspaketes 5.3.5 (Federated Learning) zur Implementierung von privatsphären-freundlichem Federated Learning auf Basis von MPC (**insgesamt +3 PM**). Diese Fähigkeit wurde zur geplanten Umsetzung des Bosch Anwendungsfalles „Battery-in-the-Cloud“ benötigt.
- Reduzierung der Arbeitspakete 5.2.2 (MLaaS Inferenz) und 5.2.3 (MLaaS Training) von 12 PM auf 3 PM (**insgesamt -9 PM**). In den verbliebenen 3 PM wurden TEE-basierte Ansätze für Inferenz und Training untersucht und prototypisch umgesetzt. Die Anwendung der kryptografischen datenschutzfreundlichen Methoden aus diesem

Arbeitspaket im Kontext des Maschinellen Lernens fanden in angepasster Form im neuen Arbeitspaket 5.3.5 statt.

- Reduktion der Arbeitspakete 5.3.2 (Automatisiertes Testwerkzeug) und 5.3.3 (Kosten- und Ressourcennutzungsmodellierung) auf 1 PM (**insgesamt -6 PM**). Die Kosten- und Ressourcennutzungsmodellierung fand in kompakterer Form in den relevanten Arbeitspaketen statt, wurde allerdings nicht automatisiert.

2.2. Wegfall Pilotanwendungsfall

Einer der beiden angedachten Pilot-Anwendungsfälle („Battery-in-the-Cloud“, BitC) konnte im Rahmen des CRYPTTECS-Projekts nicht sinnvoll weiterverfolgt werden, da der Einsatz der erarbeiteten Methoden in der Bosch-Gruppe im Projektverlauf unwahrscheinlich wurde. Der Use Case wurde daher in Absprache mit dem Projektträger fallen gelassen. Die frei gewordenen Kapazitäten wurden für die weitere Verbesserung der Carbyne-Stack-Plattform durch die Integration von Authentisierungs- und Autorisierungsfunktionen genutzt (vgl. Abschnitt 1.4.1.1).

Im Einzelnen wurden folgende Änderungen vorgenommen:

- Streichung der BitC-spezifischen Anteile (**insgesamt -6.5 PM**) in Gesamtarbeitspaket 6. Im Einzelnen:
 - AP 6.1 Definition von Evaluationskriterien für Pilotanwendungen (-0.5 PM)
 - AP 6.2 Umsetzung der Pilotanwendungen (-4 PM)
 - AP 6.3 Validierung der Pilotanwendungen (-2 PM)
- Ergänzung von Arbeitsschritten in Gesamtarbeitspaket 5 zur Erarbeitung einer Zugriffssteuerungsschicht für die Carbyne Stack Plattform (**insgesamt +6.5 PM**). Im Einzelnen:
 - AS 5.1.6: Konzeption und Umsetzung einer Authentifizierungsschicht für Carbyne Stack (3.0 PM)
 - AS 5.1.7: Konzeption und Umsetzung einer Autorisationsschicht für Carbyne Stack (3.5 PM)

2.3. Weitere Anpassungen

Auf eine ursprünglich geplante zweite Iteration der Arbeitspakete des Gesamtarbeitspakets 6 wurde aus Zeitgründen verzichtet.

Die Beauftragung eines externen Rechtsgutachtens zur Bewertung des Einsatzes der CRYPTTECS-Plattform im Kontext des „People Analytics“ Use Case hat sich verzögert, da der ursprünglich vorgesehene Auftragnehmer verstorben ist. Die dadurch notwendig gewordene Identifikation und Beauftragung eines alternativen Auftragnehmers haben zu Verzögerungen geführt. In Abstimmung mit dem Projektträger wurde daher eine aufkommensneutrale Verlängerung des Projektes um drei Monate umgesetzt.

3. Fortschritte auf dem Gebiet des Vorhabens bei anderen Stellen

In den folgenden Abschnitten werden für die Zielsetzung des CRYPTTECS-Projektes relevante Fortschritte in Wissenschaft und Forschung bei anderen Stellen skizziert, die teilweise auch zu Anpassungen des Arbeitsprogramms geführt haben (vgl. Abschnitt 2.1).

3.1. Effizientere Homomorphe Verschlüsselung

Im Bereich der homomorphen Verschlüsselung (HE) wurden während der Projektlaufzeit wesentliche Fortschritte hinsichtlich der Effizienz erzielt. Die Eignung für Hardwarebeschleunigung hat auch das Interesse der Chipindustrie geweckt, was zu einer Intensivierung der Forschungs- und Kommerzialisierungsbemühungen im Bereich HE geführt hat. Für firmenübergreifende Kooperationen, die für Bosch von Interesse sind, werden jedoch weiterhin MPC-Technologien als überlegen angesehen.

Für KI-Anwendungen, die auf Modellen mit signifikanter Größe und praxistauglicher Genauigkeit basieren, sind die Effizienzverluste beim Einsatz von HE weiterhin deutlich zu hoch. Auf die Umsetzung eines Inferenzdienstes auf Basis von HE wurde daher aufgrund mangelnder Praxistauglichkeit verzichtet (vgl. Abschnitt 1.4.2.2).

3.2. Kosteneffizientes MPC

Der Großteil der Kosten bei modernen MPC-Verfahren entsteht in der kryptografisch aufwändigen Vorverarbeitungsphase und wird maßgeblich durch die intensive Kommunikation zwischen den MPC-Parteien verursacht. Dies ist insbesondere auf die ungünstigen Preismodelle der Public-Cloud-Anbieter für Kommunikationsbandbreite zurückzuführen. Während der Projektlaufzeit hat eine Forschungslinie zum Thema *Silent MPC* (siehe z.B. [2]) an Bedeutung gewonnen. Hierbei werden sogenannte *Pseudorandom Correlation Generators* (PCGs) eingesetzt, um das Kommunikationsaufkommen bei vergleichbarer Rechenkomplexität um mehrere Größenordnungen zu reduzieren. Da dadurch die Gesamtkosten für MPC erheblich gesenkt werden können, ist dieses Forschungsgebiet für Bosch von großer Bedeutung. Das Arbeitsprogramm wurde daher um ein Arbeitspaket zu diesem Thema ergänzt (vgl. Abschnitt 1.3.1).

3.3. Verbessertes Confidential Computing

Mit der Einführung einer neuen Generation von Mikroprozessoren für Rechenzentren durch alle namhaften Hersteller (Intel, AMD, ARM) wurden die Einschränkungen früherer Generationen, insbesondere hinsichtlich des maximal verfügbaren Speicherplatzes für über Confidential Computing geschützte Prozesse, praktisch neutralisiert. Darüber hinaus bieten moderne Grafikprozessoren mittlerweile Unterstützung für Confidential Computing, sodass auch Anwendungen der Künstlichen Intelligenz und des Maschinellen Lernens unterstützt werden. In Kombination mit signifikanten Verbesserungen bei der softwareseitigen Unterstützung für Confidential Computing (zum Beispiel Confidential Containers oder Confidential Kubernetes) sind Confidential-Computing-Techniken nun breit und vergleichsweise unkompliziert einsetzbar. Aus Sicht der Bosch-Gruppe bestand daher auf diesem Gebiet kein unmittelbarer weiterer Forschungsbedarf mehr. Die entsprechenden Arbeitspakete wurden daher im Umfang deutlich reduziert (vgl. Abschnitt 1.4.2.2).

3.4. Datenschutzfreundliches Federated Learning

Federated Learning bietet im Vergleich zu zentralisierten Trainingsansätzen eine Reihe von Vorteilen. Die dezentrale Datenverarbeitung ermöglicht es, dass sensible Daten beim Dateneigner verbleiben, was bei der Bewältigung regulatorischer Herausforderungen hilfreich ist. Zudem kann die Kosteneffizienz verbessert werden, da weniger Daten über das Netzwerk transportiert werden müssen. Allerdings bietet klassisches Federated Learning keinen ausreichenden Schutz vor Angriffen, die auf die Extraktion oder Wiederherstellung der verwendeten Trainingsdaten abzielen. In den letzten Jahren wurden vermehrt Techniken zum Schutz vor solchen Angriffen erforscht. Eine dieser Techniken besteht in der Nutzung von MPC für die Aggregationsphase, also das Zusammenführen der Modellaktualisierungen der Teilnehmer. Diese datenschutzfreundliche Variante des Federated Learning ist für die weltweit operierende Bosch-Gruppe von großem Interesse. Das Arbeitsprogramm wurde daher um ein Arbeitspaket zum Thema Privacy-Preserving Federated Learning ergänzt (vgl. Abschnitt 1.4.2.4).

4. Literaturverzeichnis

- [1] Robert Bosch GmbH, „D2.1 Use Case Specification,“ 2022.
- [2] G. Couteau, Y. Ishai, L. Hohl, E. Boyle, P. Scholl und N. Gilboa, „Efficient Pseudorandom Correlation Generators from Ring-LPN,“ *Lecture Notes in Computer Science (LNCS)*, Bd. 12171, 2020.
- [3] M. Keller, „MP-SPDZ: A Versatile Framework for Multi-Party Computation,“ in *ACM SIGSAC Conference on Computer and Communications Security*, 2020.
- [4] S. Triefflinger, „PETs of the World – Unite!,“ in *Confidential Computing Mini Summit, Co-located with Open Source Summit Europe*, Bilbao, Spanien, 2023.
- [5] Robert Bosch GmbH, „Carbyne Stack Project Website,“ 09 2021. [Online]. Available: <https://carbynestack.io>. [Zugriff am 12 04 2022].
- [6] Robert Bosch GmbH, „D5.1 Concept and Design of the CRYPTTECS Platform,“ 2022. [Online]. Available: <https://drive.google.com/uc?export=download&id=1nko1yA2NtBruuSS8zauDkIPD5qTxDEpF>. [Zugriff am 12 2 2025].
- [7] Robert Bosch GmbH, „Carbyne Stack GitHub Organization,“ 2021. [Online]. Available: <https://github.com/carbynestack>. [Zugriff am 12 04 2022].
- [8] R. B. GmbH, „Carbyne Stack Klyshko Correlated Randomness Generation,“ 2022. [Online]. Available: <https://github.com/carbynestack/klyshko>. [Zugriff am 12 2 2025].
- [9] Robert Bosch GmbH, „CarbyneStackCon '23,“ 2023. [Online]. Available: <https://carbynestack.io/community/events/csc23/>. [Zugriff am 11 2 2025].
- [10] S. Triefflinger und O. Bittner, „Defense in Depth for cloud-native Computing on Encrypted Data - Stacking Confidential Computing and Secure Multiparty Computation,“ 15 10 2023. [Online]. Available: <https://blog.carbynestack.io/defense-in-depth-for-cloud-native-computing-on-encrypted-data-c265fce0184b>. [Zugriff am 13 2 2025].
- [11] S. Triefflinger, „Carbyne Stack – Towards cloud-native enterprise-grade open MPC,“ in *Cloud Native Community Meetup*, Bochum, 2023.
- [12] Robert Bosch GmbH, „Ephemeral - Carbyne Stack serverless compute service for secure multiparty computation,“ 2021. [Online]. Available: <https://github.com/carbynestack/ephemeral>. [Zugriff am 12 04 2022].
- [13] J. Liagouris, V. Kalavri, M. Faisal und M. Varia, „Secrecy: Secure collaborative analytics on secret-shared data,“ 2021. [Online]. Available: <https://arxiv.org/abs/2102.01048>. [Zugriff am 20 4 2023].
- [14] Robert Bosch GmbH, „Nettle - Privacy-Preserving Federated Learning,“ 2023. [Online]. Available: <https://github.com/carbynestack/nettle>. [Zugriff am 12 2 2025].

- [15] S. Trieflinger, „Nettle - Privacy-Preserving FL based on Flower and Carbyne Stack,“ in *Flower Summit*, Cambridge, United Kingdom,, 2023.
- [16] J. Grewe, „Continuous Load Testing using Caliper,“ in *Carbyne Stack Conference*, Renningen, Deutschland, 2023.
- [17] SAP, „ Austausch von Daten, ohne die eigentlichen Daten zu teilen: sichere Berechnungen mit Bosch und SAP,“ 2 2024. [Online]. Available: <https://news.sap.com/germany/2024/02/sichere-berechnungen-bosch-sap/>. [Zugriff am 26 4 2024].
- [18] Robert Bosch GmbH, „CarbyneStackCon '22,“ 2022. [Online]. Available: <https://carbynestack.io/community/events/csc22/>. [Zugriff am 11 2 2025].
- [19] Robert Bosch GmbH, „CarbyneStackCon '24,“ 2024. [Online]. Available: <https://carbynestack.io/community/events/csc24/>. [Zugriff am 11 2 2025].
- [20] S. Trieflinger, „Scaling the Grail - Cloud-Native Computing on Encrypted Data using Carbyne Stack,“ in *StackConf*, Berlin, Germany, 2022.
- [21] S. Trieflinger, „Carbyne Stack – Open-source cloud-native Secure Multiparty Computation,“ in *Workshop on Theory and Practice of Multi-Party Computation (TPMPC)*, Aarhus, Denmark, 2022.
- [22] S. Trieflinger, „Carbyne Stack - Cloud Native Computing on Encrypted Data,“ in *Open-Source Summit North America (OSS-NA), Emerging OS Forum*, Austin, Texas, USA, 2022.
- [23] Robert Bosch GmbH, „Carbyne Stack Medium Blog,“ 2023. [Online]. Available: <https://blog.carbynestack.io/>.
- [24] Horst Görtz Stiftung, „9. Deutscher IT Sicherheitspreis, Innovationen Gesucht,“ 2022. [Online]. Available: <https://www.deutscher-it-sicherheitspreis.de/>. [Zugriff am 20 4 2022].
- [25] „UN PET Lab Launch Press Release,“ 2022 January 2022. [Online]. Available: <https://unstats.un.org/bigdata/events/2022/unsc-un-pet-lab/UN%20PET%20Lab%20-%20Press%20Release%20-%202025%20Jan%202022.pdf>. [Zugriff am 12 04 2022].