Leistungsbeschreibung: “Encrypted Computing Compass“ - Übersicht und Machbarkeitsstudie zu Encrypted Computing

Die Cyberagentur plant verschiedene Aktivitäten für den Forschungsbereich des „Encrypted Computing“. Diese Technologien erlauben es, Daten nicht nur zu verschlüsseln, sondern auf diesen verschlüsselten Daten auch Berechnungen auszuführen. Durch den Einsatz dieser neuen Technologie ergeben sich vollkommen neue, sichere Anwendungsverfahren.

Während die prinzipielle Machbarkeiten dieser kryptographischen Techniken weitgehend geklärt ist, sind noch viele Fragen insbesondere bezüglich der Effizienz und Konkurrenzfähigkeit der Verfahren ungeklärt.

Zur Vorbereitung eines Forschungswettbewerbes zu “Encrypted Computing“ führt die Cyberagentur zunächst dieses richtungsweisende Projekt zu den verschiedenen zugrundeliegenden Technologien durch. Ziel des Projektes ist die Schaffung eines Rahmenwerks zu “Encrypted Computing“ mit Ontologie, Kategorisierung der Einsatzmöglichkeiten, Bewertung von Leistungsfähigkeit und Sicherheit sowie der anwendungsbezogene Vergleich der Verfahren.

Inhaltliche Anforderungen

Die zu erbringende Leistung als Auftragsgegenstand ist:

Nr.	Anforderung
1.	**Ontologie und Definition** a) Erstellung einer Ontologie der verschiedenen Bereiche von “Encrypted Computing” mit wissenschaftlicher Arbeitsweise. b) Insbesondere die Konzepte Fully Homomorphic Encryption, Indistinguishability Obfuscation und Secure Multiparty Computation und deren Beziehung zueinander sowie deren Kombination müssen hierbei Beachtung finden. c) Diese Aufführung müssen sowohl Ähnlichkeiten als auch Unterschiede dieser Konzepte klarstellen. d) Hierfür ist es weiterhin notwendig die zugrundeliegenden kryptographischen Methoden und Schemata im Detail zu klassifizieren. e) Ein Überblick über internationale Forschungsgruppen und Budgets, welche das Thema „Encrypted Computing“ aktuell bearbeiten, muss erarbeitet werden.
2.	**Verfahren und Use Cases** a) Auf der Ontologie aufbauend, muss eine Datenbank zu Anwendungen aktueller “Encrypted Computing” Ansätze erstellt werden. b) Es müssen elementare Use-Cases für „Encrypted Computing“- Verfahren identifiziert werden (auch und beispielsweise für “Machine Learning”). c) Es muss eine Vergleichsmatrix der Ansätze bezüglich der Use-Cases angefertigt werden. d) Aktuelle Limitierungen müssen dargelegt werden, bei denen sich auf absehbare Zeit (5-15 Jahre) die Anwendung aus wissenschaftlicher Sicht nicht lohnt.
3.	**Bedrohungsmodelle** a) Es müssen verschiedene Bedrohungsmodelle von “Encrypted Computing”-Verfahren erläutert werden. b) Die Sicherheitsgarantien und -grenzen der Verfahren müssen dargelegt werden.

4.	**Sicherheitseigenschaften** a) Ein Survey der Sicherheitsdefinitionen und der Sicherheitsannahmen von „Encrypted Computing“- Verfahren muss erstellt werden. b) Anführen von Analysen bzw. Beweise der Sicherheit von „Encrypted Computing“-Verfahren (hier z.B. Sicherheitsanalysen und -vergleiche, Analysen der Post-Quanten-Sicherheit) muss erfolgen. c) Im konkreten Fall von FHE beispielsweise ist nicht nur die Sicherheit des Verschlüsselungsverfahrens relevant für die Sicherheit von Anwendungen, sondern auch die Korrektheit des Verfahrens.
5.	**Benchmarking** a) Die verschiedenen Ansätze müssen vergleichbar gemacht und verglichen werden, dazu müssen die Metriken für die Performanz (Chiffratgröße, Berechnungsaufwand etc.) und Sicherheit (Plausibilität von Annahmen) erstellt und genutzt werden. b) Software muss entwickelt werden, welche es erlaubt, die Leistungsfähigkeit von „Encrypted Computing“-Verfahren zu ermitteln (z.B. Laufzeiten, Speicherplatzbedarf, Parallelisierbarkeit). c) Verschiedene Varianten von Fully Homomorphic Encryption (Multikey FHE, Split FHE, approximate FHE) müssen verglichen werden. d) Die Anwendbarkeit auf die verschiedenen Use Cases muss evaluiert (Benchmark) werden.

Nicht-funktionale Anforderungen

Es gelten folgende weitere Bedingungen:

Nr.	Anforderung
6.	**Form und Umfang** a) Der Output muss sich hinsichtlich der Form am Standard von Publikationen in wissenschaftlichen Journals orientieren. b) Der Umfang des Dokumentes muss die Projektlaufzeit und den darin geforderten Arbeiten entsprechend repräsentieren. c) Ein von wissenschaftlicher Expertise geprägter Arbeitsansatz muss dargelegt werden.
7.	**Sprache und Darstellung** a) Die Sprache des Outputs ist Deutsch oder Englisch. Sie muss einerseits in einer für die wissenschaftliche Community aussagekräftigen Ausdrucksweise, andererseits in einer für fachfremde Personen verständlichen Art erfolgen. b) Die Darstellung von Text und Visualisierung muss so erfolgen, dass das Dokument ohne großen weiteren Aufwand durch die Cyberagentur gemeinsam mit den Autoren veröffentlicht werden kann.
8.	**Eignung zur Publikation** a) Eine Veröffentlichung des Ergebnisdokuments hat gemeinsam durch die Cyberagentur und die Autoren (Auftragnehmer) zu erfolgen. b) Weitere wissenschaftliche Veröffentlichung (z.B. Konferenz) müssen in Absprache und Einwilligung mit dem Auftraggeber erfolgen.
9.	**Referenzen** a) Referenzierte Quellen, wissenschaftliche Erkenntnisse, Richtlinien etc. müssen in einer einheitlichen und gebräuchlichen Zitierweise aufbereitet werden.
10.	**Weiterentwicklung** a) Das Dokument und die entwickelte Software muss so aufgebaut sein, dass dies kontinuierlich überarbeitet und/oder ergänzt werden kann.
11.	**Nutzbarkeit**

	a) Projektergebnisse werden von Agentur verwertet werden. Weitere Nutzung darf nur mit Einwilligung des Auftraggeber erfolgen.

Anforderungen an den Auftragnehmer und Projektrealisierung

Nr.	Anforderung
12.	Der Auftragnehmer muss qualitative Referenzen in der wissenschaftlichen Forschung im Bereich „Encrypted Computing“ vorweisen und belegen.
13.	Der Auftragnehmer muss die Kompetenz im Bereich „Encrypted Computing“ im für das Projekt vorgeschlagene Team nachweisen.
14.	Der Auftragnehmer muss nachweisen, dass er auf ein fundierten wissenschaftliches Netzwerk im Bereich „Encrypted Computing“ zurückgreifen kann.
15.	Die Durchführungszeit darf nicht länger als 9 Monate nach Projektstart betragen.

Bewertung der Zuschlagskriterien

Nr.	Kriterium	Punkte (1-5)	Gewichtung
1	Inhaltliche Anforderungen		30 %
	5 Pkt = Es ist erkennbar, dass die Anforderungen 1-5 in Gänze einbezogen und erfüllt werden.		
	0 Pkt = Es ist nicht erkennbar, dass die Anforderungen 1-5 erfüllt werden.		
2	Nicht-funktionale Anforderungen		20 %
	5 Pkt = Es ist erkennbar, dass die Anforderungen 5-11 in Gänze einbezogen und erfüllt werden.		
	0 Pkt = Es ist nicht erkennbar, dass die Anforderungen 5-11 erfüllt werden.		
3	Anforderungen an den Auftragnehmer		20 %
	5 Pkt = Es ist erkennbar, dass die Anforderungen 12-15 in Gänze einbezogen und erfüllt werden.		
	0 Pkt = Es ist nicht erkennbar, dass die Anforderungen 12-15 erfüllt werden.		
4	Preis		30 %

Eine Abstufungen bei der Punktevergabe für Nummer 1-3 erfolgt, wenn nur Teile der Anforderungen erfüllt wurden.