Computación Multi-Parte en la Administración: Prueba de Concepto de Concesión de Becas en el Gobierno Vasco

Julen Bernabé-Rodríguez
TECNALIA, Basque Research and Technology Alliance (BRTA)
Derio, España
julen.bernabe@tecnalia.com

Oscar Lage
TECNALIA, Basque Research and Technology Alliance (BRTA)
Derio, España
oscar.lage@tecnalia.com

Oscar Guadilla Jiménez
Sociedad Informática del Gobierno Vasco – EJIE
Vitoria, España
o-guadilla@ejie.eus

Borja Urquizu
TECNALIA, Basque Research and Technology Alliance (BRTA)
Derio, España
borja.urquizu@tecnalia.com

Iván Gutiérrez-Agüero
TECNALIA, Basque Research and Technology Alliance (BRTA)
Derio, España
ivan.gutierrez@tecnalia.com

Endika Gandarias Blanco
Sociedad Informática del Gobierno Vasco – EJIE
Vitoria, España
e-gandarias@ejie.eus

Resumen - Este trabajo aborda la necesidad de interoperabilidad en la prestación de servicios públicos y cómo, a pesar de su valor, el Esquema Nacional de Interoperabilidad (ENI) en España presenta limitaciones. Se discute cómo la consulta de datos en administraciones terceras a través de servicios web acordados presenta desafíos, especialmente cuando los cambios en las políticas de consulta requieren modificaciones extensas de datos personales considerados como sensibles por la legislación actual. Además, en esta línea, se presenta una solución de interoperabilidad basada en computación multi-parte, así como una prueba de concepto de esta para la concesión de becas en el Gobierno Vasco. El documento describe las limitaciones y resultados de dicha prueba de concepto, y también diferentes líneas de investigación identificadas. Se espera que este trabajo fomente la discusión sobre cómo mejorar la interoperabilidad y la eficiencia en la prestación de servicios públicos, sobre todo cuando dicha interoperabilidad involucra datos sensibles.

Index Terms **- computación multi-parte, privacidad, criptografía, RGPD, Administración Pública**

Tipo de contribución: *Transferencia. Proyectos de I+D realizados con usuarios finales de tecnología (límite 8 páginas)*

I. INTRODUCCIÓN

La prestación de servicios públicos a menudo requiere de una interoperabilidad efectiva entre las diferentes administraciones públicas para poder resolver un expediente o una consulta. Esta necesidad se ha vuelto cada vez más evidente en la era digital, donde la eficiencia y la rapidez son esenciales para satisfacer las expectativas de los ciudadanos.

En España, el Esquema Nacional de Interoperabilidad (ENI) se estableció para definir las condiciones de interoperabilidad y de seguridad que deben reunir los sistemas y soluciones utilizados por las administraciones públicas. Sin embargo, los servicios que actualmente cubre el ENI son limitados y las implementaciones existentes no son suficientes para resolver la totalidad de las casuísticas a las que se enfrenta la Administración. Además, la interoperabilidad entre administraciones públicas se vuelve mucho más complicada cuando los datos a compartir son potencialmente sensibles según la normativa aplicable en materia de protección de datos de carácter personal [1], entre las que la Agencia Española de Protección de Datos (AEPD) incluye [2] el Reglamento (UE) 2016/679 (RGPD) [3] y la Ley Orgánica 3/2018 (LOPDGDD) [4].

La interoperabilidad y consulta de datos en administraciones terceras se ha establecido en muchos casos mediante la implementación de servicios web acordados por las diferentes administraciones para la consulta autenticada de datos. Sin embargo, este enfoque presenta un problema de base para las administraciones en cuanto a la responsabilidad de gestión técnica de datos y el cumplimiento con el principio de minimización (artículo 5.1.c del RGPD) de datos en la provisión de servicios previsto en las leyes. Este principio tiene el objetivo de limitar las prácticas de recolección, procesamiento y almacenamiento de datos personales, siempre que se pueda evitar.

En este contexto, la posibilidad de tener un repositorio virtual de información sobre el ciudadano, que respete las políticas de protección de datos actuales ([3], [4]) podría ser muy beneficioso para la Administración. Este enfoque

fomentaría la interoperabilidad, permitiría una mejor explotación de datos y mejoraría el servicio al ciudadano, entre otros beneficios. Sin embargo, también presenta retos tecnológicos significativos en términos de ciberseguridad que deben ser abordados y que se pretenden abordar en el presente trabajo.

Este trabajo se centra en la necesidad de interoperabilidad en la prestación de servicios públicos y cómo el Esquema Nacional de Interoperabilidad (ENI) en España [5], aunque valioso, tiene limitaciones en su alcance y servicios. Se discute cómo la consulta de datos en administraciones terceras a través de servicios web acordados presenta desafíos, especialmente cuando los cambios en las políticas de consulta requieren modificaciones extensas de datos sensibles. Se propone una plataforma criptográfica de intercambio de información sobre el ciudadano/empresa, que respeta la legislación de privacidad actual, como una solución potencial. Además, se presenta una prueba de concepto real de computación multi-parte (MPC) en la administración pública, específicamente en la concesión de becas en el Gobierno Vasco. La estructura del documento se presenta de la siguiente manera: la Sección II aborda los antecedentes tecnológicos y normativos del proyecto, la Sección III presenta la arquitectura de la solución a validar, y la Sección IV presenta las conclusiones de la prueba de concepto, discutiendo los resultados de la transferencia de conocimiento y reflexionando sobre los retos y barreras para adoptar este tipo de soluciones criptográficas para resolver el desafío de la interoperabilidad en la administración pública.

II. Antecedentes

A. Computación Multi-Parte

El pilar fundamental de la solución para garantizar la privacidad de los solicitantes durante los procesos de concesión de becas es la computación multi-parte. MPC permite que un conjunto de n participantes realice un cálculo arbitrario utilizando sus datos privados, incluso si algunos de ellos son corruptos. Esta tecnología permite a los participantes conocer el resultado de la ejecución, garantizando que no se pueda inferir ninguna información extra excepto la derivada de dicho resultado.

Debido a su naturaleza descentralizada, en la literatura es habitual definir al adversario como una entidad capaz de corromper a algunos de los participantes [6]. Los adversarios capaces de hacer que los participantes se salgan de la ejecución MPC se denominan *maliciosos*, mientras que aquellos que sólo pueden aprender de sus datos, pero no pueden desviarse del protocolo se denominan *semi-honestos*. Se dice que una red MPC es una red de *mayoría honesta* si el adversario no puede corromper a más de la mitad de los participantes. Si el adversario puede corromper hasta $n-1$ participantes, se dice que es una red MPC de *mayoría deshonesta*.

En la actualidad, existen multitud de protocolos MPC en la literatura. Entre los protocolos seguros frente a una mayoría deshonesta de adversarios maliciosos, cabe destacar LowGear [7], HighGear [7], y TopGear [8], todos ellos protocolos basados en cifrados homomórficos. El protocolo MASCOT [9] también garantiza el mismo nivel de seguridad, pero basándose en *oblivious transfer*. Los protocolos seguros frente a una mayoría honesta de adversarios maliciosos normalmente están basados en la compartición de secretos de Shamir [10], derivando en diferentes protocolos MPC como los presentados en [11], [12], [13]. En cuanto a los protocolos MPC seguros frente a una mayoría deshonesta de adversarios semi-honestos, es posible reducir la seguridad de los protocolos LowGear, HighGear, TopGear e incluso MASCOT para adecuarlos a esta casuística. En cualquier caso, uno de los protocolos más eficientes en este ámbito es el propuesto por Cramer et al. en [14]. De forma similar, es posible aplicar la compartición de secretos de Shamir para construir protocolos seguros frente a una mayoría honesta de adversarios semi-honestos, resultando en protocolos como los propuestos en [12], [13], [15].

En cuanto a la implementación, actualmente, hay varios proyectos de código abierto en curso [16]. Sin embargo, uno de los *frameworks* más avanzados en este ámbito es MP-SPDZ [17]. Este framework permite ejecutar diferentes protocolos MPC según el nivel de seguridad deseado para números arbitrarios de participantes. En efecto, MP-SPDZ incluye implementaciones de los protocolos HighGear, LowGear, MASCOT, Shamir Malicioso [11], etc. Este repositorio, además, se encuentra en un estado mucho más avanzado que el de otras opciones.

B. Contexto Normativo

La Estrategia de Mercado Único Digital [18] puso en marcha el Plan de Acción sobre Administración Electrónica de la Unión Europea (UE) 2016-2020 [19] para acelerar la transformación digital en la administración. En el marco de dicha estrategia, se establecen una serie de principios que cualquier iniciativa posterior debería respetar. De especial relevancia son tres de ellos: “Fiabilidad y seguridad”, “Apertura y transparencia” e “Interoperabilidad por defecto”. Puesto que el intercambio o compartición de información previsto en los objetivos estratégicos establecidos supone en todas sus formas un tratamiento de datos, estas acciones se deben encontrar al amparo de la normativa comunitaria y nacional [20].

Esquema Nacional de Interoperabilidad (ENI)

El ENI es un marco normativo español que establece las condiciones de interoperabilidad y seguridad que deben reunir los sistemas y soluciones utilizados por las administraciones públicas. Su objetivo es garantizar un adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las administraciones públicas. El ENI se materializa en el Real Decreto 4/2010 [21] y se acompaña de una serie de Normas Técnicas de Interoperabilidad que desarrollan aspectos concretos de la interoperabilidad entre las administraciones públicas y con los ciudadanos.

Reglamento sobre la Europa Interoperable

Esta norma europea [22] tiene como objetivo asegurar el flujo de datos y la coordinación de los servicios digitales en el ámbito del sector público de la UE, a fin de garantizar la fluidez de la prestación transfronteriza de servicios públicos [23]. Propone la creación de una red de administraciones públicas

digitales interconectadas y la aceleración de la transformación digital del sector público europeo.

Legislación Relativa a la Protección de Datos Personales

El RGPD es una norma europea que protege los datos personales de los ciudadanos de la UE. Establece las condiciones bajo las cuales se pueden recoger, procesar y almacenar los datos personales, y otorga a los ciudadanos un mayor control sobre sus datos personales mediante los derechos a ARCO-POL. La LOPDGDD deroga la anterior LOPD para adaptar la ley española a los requisitos del RGPD y compartiendo su mismo régimen sancionador, de aplicación a entidades que operen en territorio español [2].

C. Caso de estudio: Concesión de Becas de Educación en el Gobierno Vasco

El proceso de solicitud de becas para la realización de estudios universitarios promovida por el Departamento de Educación de Gobierno Vasco [24] se realiza mediante convocatoria pública atendiendo a normativa publicada en el Boletín Oficial del País Vasco [25]. El proceso requiere agregar información que debe ser recogida de distintos departamentos, en su mayor parte de carácter personal.

1. Departamento de Educación y Universidades: datos relacionados con los estudios a realizar.
2. Diputaciones Forales: datos generales relacionados con la persona solicitante y sus progenitores.
3. Departamento de Economía y Hacienda: datos económicos sobre los progenitores.

Bajo los mecanismos actuales, las administraciones se encuentran con el reto de interoperar de forma efectiva mientras se respetan los derechos del ciudadano [26], [27]. Este reto está limitado por las capacidades técnicas del estado del arte, que requiere medidas innovadoras que promuevan un intercambio de conocimiento confiable y que atienda a la privacidad del ciudadano.

Este proceso de solicitud de becas plantea unas condiciones donde se computa el cumplimiento de requisitos sobre los datos privados de la persona solicitante y su unidad convivencial. MPC se identifica como respuesta a esta computación con datos de carácter personal que no pueden ser compartidos con otras fuentes siempre que sea posible.

III. Análisis Exploratorio

A. Contextualización y Arquitectura

Con el objetivo de dar solución parcial (sólo se han resuelto algunos de los requisitos asociados a la concesión de becas, no todos ellos) a la mejora de la interoperabilidad entre administraciones públicas durante un proceso de concesión de becas en el País Vasco, se ha desarrollado una prueba de concepto que habilita el intercambio de datos sensibles (pertenecientes al solicitante y sus progenitores) *ipso facto* entre las diputaciones de la Comunidad Autónoma Vasca y el Departamento de Educación y Universidades, mediante el uso de la tecnología MPC.

Más concretamente, la prueba de concepto consiste en la resolución de los requisitos para la concesión de becas [25] asociados a los datos que tienen las propias diputaciones. Por tanto, los requisitos a resolver en la prueba de concepto se recogen en la Tabla 1:

ID	Requisito	Propietario del dato
G01	Estar empadronado/a en el País Vasco.	Diputaciones
G02	Tributar en el País Vasco.	Diputaciones
E03	No superar el umbral máximo de renta.	Diputaciones
E04	No superar los 1.700 euros en rendimientos (+/-) netos reducidos del capital mobiliario.	Diputaciones

Tabla 1. Requisitos en la concesión de becas asociados a las diputaciones.

Nótese que únicamente se han resuelto los requisitos asociados con los datos que poseen las diputaciones, y no los asociados con otros departamentos, como el Departamento de hacienda y Economía. A este respecto, a pesar de que en la Tabla 1 se establezca como propietarias del dato a las diputaciones, se asume que la propietaria del dato será alguna de las tres, y no todas. A modo de ejemplo, para el requisito G01, una persona únicamente puede estar empadronada en una de las tres provincias, y no en varias a la vez. Esto ocurre de forma similar para los otros requisitos. Para la resolución de los requisitos asociados a las diputaciones, se propone la arquitectura de red que se muestra en la Figura 1.

Como se puede observar en la Figura 1, es necesario que, tanto el Departamento de Educación y Universidades, como cada una de las diputaciones, despliegen una aplicación que contenga un agente MPC con acceso a los datos. Este agente MPC encapsula las funcionalidades del framework MP-SPDZ. Cada una de las diputaciones accede a dicha aplicación a través de la interfaz de usuario (UI).

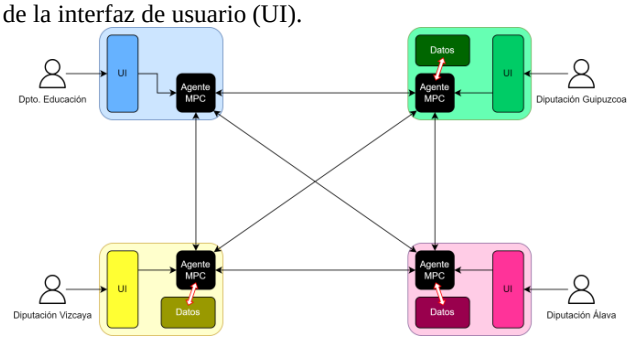

Figura 1. Arquitectura de la solución.

Es importante mencionar que, para el desarrollo de la prueba de concepto, se ha asumido que la persona solicitante ha realizado previamente la solicitud a la beca. En esta solicitud, únicamente sería necesario aportar el Documento Nacional de Identidad (DNI). Con este documento, las diputaciones pueden deducir localmente los datos necesarios para comprobar si se cumplen los requisitos de la Tabla 1.

Obsérvese que, sin computación multi-parte, las diputaciones deben cruzar datos en claro con el fin de comprobar los requisitos. A modo de ejemplo, si la persona solicitante está empadronada en Guipúzcoa, la Diputación de Vizcaya es incapaz de saber si está empadronada en el País Vasco, a no ser que la Diputación de Guipúzcoa le facilite dicha información.

Un aspecto a destacar de la arquitectura definida en la Figura 1 es el hecho de que todos los agentes MPC han de saber la localización de los demás agentes. Si los agentes MPC no se

conocen entre ellos, no es posible realizar ejecuciones con la librería MP-SPDZ.

B. Aspectos Técnicos de la Implementación y Resultados Obtenidos

La implementación de la prueba de concepto se ha llevado a cabo utilizando cuatro máquinas virtuales desplegadas en Amazon Web Services (AWS) provistas por EJIE (Sociedad Informática del Gobierno Vasco). Cada una de las máquinas emplea 2 CPU y 4GB de memoria RAM, corriendo en Ubuntu 20.04. Además, las máquinas exponen el puerto 5000; es este puerto el que usan los agentes MPC a fin de efectuar las comunicaciones necesarias entre ellos durante las ejecuciones.

Para cada uno de los requisitos a resolver, se ha implementado y compilado un algoritmo diferente. Es por ello que el propio cliente deberá seleccionar el requisito a resolver en la UI, antes de comenzar la ejecución. Estos algoritmos se han escrito en el lenguaje nativo existente en la librería MP-SPDZ, que es similar a Python. Dependiendo del requisito a resolver, los algoritmos permiten varias entradas de datos. Este es el caso de los dos últimos requisitos en la Tabla 1, que operan con los datos de los progenitores, y éstos pueden variar dependiendo de si la declaración de la renta se realiza de forma individual o conjunta.

Tal y como se introdujo en la Sección II.A. MP-SPDZ permite compilar los mismos algoritmos sobre diferentes protocolos MPC. Por esta razón, en la implementación, se han seleccionado 4 protocolos (uno por cada nivel de seguridad) que pueden emplearse indistintamente a la hora de efectuar las ejecuciones:

- Mayoría deshonesta de adversarios maliciosos: MASCOT [9].
- Mayoría honesta de adversarios maliciosos: Shamir Malicioso [11].
- Mayoría deshonesta de adversarios semi-honestos: Cramer et al. [14].
- Mayoría honesta de adversarios semi-honestos: Shamir [11].

La elección de estos protocolos frente a otras alternativas se debe principalmente a ciertas ventajas que estos protocolos presentan. En efecto, el protocolo MASCOT es el único en su nivel de seguridad que no requiere de un proceso previo de generación de claves, pudiendo realizar las ejecuciones en un tiempo. Esto no es posible en protocolos como LowGear o HighGear. El protocolo de Shamir Malicioso en [11] resulta ser el único protocolo con este nivel de seguridad que permite realizar ejecuciones con números arbitrarios de participantes (las otras opciones sólo están implementadas para 3 participantes). Esto mismo ocurre en su versión para adversarios semi-honestos. Por último, el protocolo propuesto por Cramer et al. en [14] es, con diferencia, el más eficiente en su nivel de seguridad. Es importante remarcar que se recomienda emplear únicamente los dos primeros protocolos, ya que los otros niveles de seguridad pueden ser demasiado laxos en ciertas situaciones.

Con el fin de que las ejecuciones se realizaran correctamente, ha sido necesario realizar un procesado previo de los datos, con el fin de normalizarlos y de darles el mismo formato en todas las diputaciones. Los datasets empleados han sido de tipo CSV, cada dataset conteniendo los atributos que las diputaciones guardan de cada uno de sus ciudadanos. Este dataset es por tanto, de tamaño reducido y fácil de manejar.

A partir de esta configuración, los resultados obtenidos han sido muy satisfactorios. En efecto, la prueba de concepto ha permitido demostrar la viabilidad de resolver la comprobación de los requisitos empleando MPC. Esta tecnología ha habilitado el intercambio de los datos de las diferentes diputaciones y la obtención de un resultado conjunto en pocos segundos, mientras se asegura la privacidad de los datasets introducidos por cada una de las diputaciones. Tal y como era de esperar, a mayor seguridad del protocolo, el tiempo de ejecución y los recursos empleados también son mayores. Es por ello que el protocolo de Shamir Malicioso, teniendo un nivel de seguridad suficiente para esta prueba de concepto, ha resultado ser el protocolo idóneo para dar solución a la prueba de concepto.

Esta solución, no obstante, ha sacado a relucir ciertos inconvenientes de la tecnología MPC que merecen tenerse en cuenta. Los principales inconvenientes encontrados son:

- Las ejecuciones requieren de sincronía por parte de todos los participantes. Esto significa que, si una de las diputaciones o el Departamento de Educación y Universidades falla antes o durante la ejecución, entonces el resultado también es fallido.
- Todos los participantes han de conocerse previamente a realizar las ejecuciones MPC. Es decir, si hubiera que añadir un nuevo participante a la red, todos los participantes anteriores tendrían que saber dónde se encuentra éste, y actualizar su configuración.
- Las ejecuciones se han realizado siempre sobre datasets y participantes limitados. En consecuencia, no se ha probado cómo escala este tipo de soluciones en términos de estas dos variables. No obstante, existen evidencias de que ambos protocolos, y principalmente MASCOT, escalan de forma deficiente en ambos casos [28].

IV. Conclusiones

Este estudio aborda la necesidad de interoperabilidad en la prestación de servicios públicos y presenta una solución potencial a través de MPC. Tras analizar los últimos avances en Privacy Preserving Computing, se ha evaluado la idoneidad de la tecnología MPC para compartir y operar datos sin necesidad de revelarlos entre las partes. Se ha estudiado la viabilidad de implementar esta tecnología en la Administración Pública utilizando la infraestructura de EJIE (Sociedad Informática del Gobierno Vasco).

Para probar la tecnología, se identificó el caso de uso de concesión de becas del Departamento de Educación, que implica la comunicación entre diferentes departamentos de las administraciones. Se han probado diferentes configuraciones de protocolos de computación multi-parte disponibles, siendo los protocolos en [9] y [11] los que han mostrado un mejor comportamiento, garantizando un nivel de seguridad suficiente.

Se han realizado diferentes ejecuciones sobre datos de distintas entidades o departamentos, incluyendo la verificación de padrón, rendimiento del capital inmobiliario de uno o dos ciudadanos, tributación en País Vasco, y umbral de renta obtenida por un ciudadano. La infraestructura ha quedado fijada a cuatro entidades, siendo éstas: las tres diputaciones vascas y el Departamento de Educación y Universidades. No

se ha analizado cómo afectaría un crecimiento de los participantes a los tiempos de ejecución y recursos necesarios, aunque se tienen evidencias de que afectaría negativamente [28].

Entre las limitaciones del estudio cabe destacar que el tamaño del dataset ha sido limitado. En futuras pruebas, se debería probar la escalabilidad de la solución con un dataset realista de varios GBs, así como extrapolar medidas de escalabilidad de la tecnología en función de la complejidad de las funciones a ejecutar y del tamaño de la muestra.

La tecnología actual requiere que la ejecución sea un proceso síncrono y se echa en falta un orquestador que ejecute el algoritmo. Es más, poder ejecutar varias ejecuciones encadenadas para resolver problemas complejos que requieran operaciones sobre diferentes fuentes sería una funcionalidad deseada en dicho orquestador. Por otro lado, debido al diseño actual, en el que se requiere de un preprocesado de los datos antes de la propia ejecución, en el caso de agregar valores nuevos no numéricos, se requiere modificar dicho preprocesamiento. La tecnología no facilita la integración de las fuentes de datos, por lo que se requiere una implementación y solución expresa para ello.

El estudio también identifica varias líneas de investigación futuras que podrían abordar los desafíos actuales en la implementación de la tecnología de computación multi-parte en la administración pública.

En primer lugar, se deben desarrollar soluciones tecnológicas que faciliten la interoperabilidad de los datos. Actualmente, las tecnologías disponibles requieren que todos los participantes conozcan la información sobre el dataset a tratar y adaptar los algoritmos al mismo. Esto puede ser un obstáculo para la implementación eficiente de la tecnología MPC, especialmente en entornos donde la información puede ser sensible o confidencial.

Además, se debe analizar cómo se gestiona y gobierna este tipo de espacios de datos criptográficos por los usuarios finales. Las soluciones actuales requieren de una codificación *ad-hoc* al caso y no existen herramientas de gestión y administración de las mismas adaptadas a las necesidades de los administradores de los centros de cálculo de las administraciones públicas o grandes empresas. La falta de tales herramientas puede dificultar la adopción y el uso efectivo de la tecnología MPC en estos entornos. Por lo tanto, la investigación futura debería centrarse en abordar estos desafíos para facilitar la adopción y la implementación efectiva de la tecnología MPC en la administración pública. Al hacerlo, se puede avanzar hacia la resolución del gran reto de la interoperabilidad entre administraciones y mejorar la eficiencia en la prestación de servicios públicos.

Cabe señalar que este trabajo puede ser de gran interés para investigadores que estén identificando líneas de investigación en criptografía aplicada, así como para *practitioners* que quieran conocer los beneficios y limitaciones actuales de la tecnología en su implementación en la administración pública para la resolución del gran reto de la interoperabilidad entre administraciones. Esperamos que este trabajo contribuya a la comprensión y adopción de la computación multi-parte en la administración pública y fomente la discusión sobre cómo mejorar la interoperabilidad y la eficiencia en la prestación de servicios públicos.

REFERENCIAS

[1] M. de Hacienda del Gobierno Español, “Normativa sobre Datos Personales.” 2022. [Online]. Available: https://www.hacienda.gob.es/es-ES/El%20Ministerio/Paginas/DPD/Normativa_PD.aspx

[2] A. E. de Protección de Datos, “Protección de Datos.” 2022. [Online]. Available: https://www.aepd.es/informes-y-resoluciones/normativa

[3] P. y Consejo Europeo, “Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.” 2016. [Online]. Available: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[4] J. del Estado, “Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, 6 de diciembre de 2018, nº 294.” 2018. [Online]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[5] PAe, “Esquema Nacional de Interoperabilidad - ENI,” www.administracionelectronica.gob.es.

[6] Y. Lindell, “Secure multiparty computation,” *Commun ACM*, vol. 64, no. 1, pp. 86–96, 2020.

[7] M. Keller, V. Pastro, and D. Rotaru, “Overdrive: making SPDZ great again,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2018, pp. 158–189.

[8] C. Baum, D. Cozzo, and N. P. Smart, “Using TopGear in overdrive: a more efficient ZKPoK for SPDZ,” in *International Conference on Selected Areas in Cryptography*, 2019, pp. 274–302.

[9] M. Keller, E. Orsini, and P. Scholl, “MASCOT: faster malicious arithmetic secure computation with oblivious transfer,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 830–842.

[10] A. Shamir, “How to share a secret,” *Commun ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[11] R. Cramer, I. Damgård, and U. Maurer, “General secure multi-party computation from any linear secret-sharing scheme,” in *International Conference on the Theory and Applications of Cryptographic Techniques*, 2000, pp. 316–334.

[12] D. Chaum, C. Crépeau, and I. Damgard, “Multiparty unconditionally secure protocols,” in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, in STOC ’88. New York, NY, USA: Association for Computing Machinery, 1988, pp. 11–19. doi: 10.1145/62212.62214.

[13] D. and H. K. and I. D. and K. R. and L. Y. and N. A. Chida Koji and Genkin, “Fast Large-Scale Honest-Majority MPC for Malicious Adversaries,” in *Advances in Cryptology – CRYPTO 2018*, A. Shacham Hovav and Boldyreva, Ed., Cham: Springer International Publishing, 2018, pp. 34–64.

[14] R. Cramer, I. Damgård, and J. B. Nielsen, “Multiparty computation from threshold homomorphic encryption,” in *Advances in Cryptology—EUROCRYPT 2001: International Conference on the Theory and Application of Cryptographic Techniques Innsbruck, Austria, May 6–10, 2001 Proceedings 20*, 2001, pp. 280–300.

[15] V. Goyal, H. Li, R. Ostrovsky, A. Polychroniadou, and Y. Song, “ATLAS: efficient and scalable MPC in the honest majority setting,” in *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part II 41*, 2021, pp. 244–274.

[16] D. Rotaru, “Awesome MPC.” GitHub, 2023. [Online]. Available: https://github.com/rdragos/awesome-mpc

[17] M. Keller, “MP-SPDZ: A versatile framework for multi-party computation,” in *Proceedings of the 2020 ACM SIGSAC conference on computer and communications security*, 2020, pp. 1575–1590.

[18] C. Europea, “Una Estrategia para el Mercado Único Digital de Europa. COM 192 final.” 2015. [Online]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0192&rid=1

[19] C. Europea, “Plan de Acción sobre Administración Electrónica de la UE 2016-2020. COM 179 final.” 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016DC0179

[20] J. P. Córdoba, “Interoperabilidad e intercambio de datos entre administraciones públicas.,” *Revista General de Derecho Administrativo*, no. 62, p. 14, 2023.

[21] M. de la Presidencia del Gobierno Español, “Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

«BOE» núm. 25, de 29/01/2010.” 2010. [Online]. Available: https://www.boe.es/eli/es/rd/2010/01/08/4/con

[22] C. Europea, “Ley sobre la Europa Interoperable. COM 720 final.” 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX%3A52022PC0720

[23] F. Pflücke, “Interoperability in the EU: Paving the Way for Digital Public Services,” *SSRN Electronic Journal*, 2023, doi: 10.2139/ssrn.4561014.

[24] G. Vasco, “Becas para realizar estudios universitarios y otros estudios superiores.” 2023. Accessed: Mar. 12, 2024. [Online]. Available: https://www.euskadi.eus/alumnado-universitario-becas-estudios-universitarios-y-otros-superiores/web01-a3lagun/es/

[25] D. de Educación del País Vasco, “ORDEN de 20 de junio de 2023, del Consejero de Educación, por la que se convocan becas para realizar estudios universitarios y otros estudios superiores en el año académico 2023-2024, y ayudas destinadas a sufragar los gastos de transporte para estudiantes con discapacidad física o psíquica y especiales dificultades de movilidad.” 2023. Accessed: Mar. 12, 2024. [Online]. Available: https://www.euskadi.eus/web01-bopv/es/bopv2/datos/2023/06/2303124a.pdf

[26] D. U. Galetta, “Public Administration in the Era of Database and Information Exchange Networks: Empowering Administrative Power or Just Better Serving the Citizens?,” *European Public Law*, vol. 25, no. 2, pp. 171–181, 2019, [Online]. Available: https://kluwerlawonline.com/journalarticle/European+Public+Law/25.2/EURO2019012

[27] K. Bovalis *et al.*, “Promoting Interoperability in Europe’s E-Government,” *Computer (Long Beach Calif)*, vol. 47, no. 10, pp. 25–33, 2014, doi: 10.1109/MC.2014.295.

[28] J. Bernabé-Rodríguez, C. Regueiro Senderos, and I. Seco Aguirre, “Ampliando los límites de MP-SPDZ,” *JNIC 2023: VIII Jornadas Nacionales en Investigación en Ciberseguridad (2023)*, 2023.