Institution: University of Bristol		
Unit of Assessment: 11) Computer Science and Informatics		
Title of case study: Securing Data During Computation: Turning Theory into Practice		
Period when the underpinning research was undertaken: 2007 - 2019		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Nigel Smart	Professor of Cryptology	2000 - 2020
Period when the claimed impact occurred: 1st August 2013 – 2020		
Is this case study continued from a case study submitted in 2014? No		

1. Summary of the impact

Against a backdrop of increased public and governmental scrutiny of data privacy standards, University of Bristol research in Multi-Party Computation (MPC) and Fully Homomorphic Encryption (FHE) have allowed, for the first time, the computation of data without revealing its contents to the parties which are performing the computation. This has allowed for responsible innovation of new services and products through its central role in the establishment of spin-outs and start-ups, such as Cosmian, Duality, Enveil, Galois, Partisia, Sepior, Unbound Tech and Zama. In addition, large companies and governments have adopted the technology in applications and proofs-of-concept. MPC is stimulating evidence-based policy practice and debate in issues with a privacy dimension, such as census data, leading to the creation of a US White House report on inter-agency data sharing and UN guidelines on preserving privacy.

2. Underpinning research

In the mid 2000's the work of Smart at the University of Bristol presented the first practical and fully secure realisations of Multi-Party Computation and Fully Homomorphic Encryption. This led to an explosion of interest and investment by governments, funding agencies and, eventually, venture capitalists. The goal of this technology is to secure data during computation, as opposed to the traditional areas of securing data-in-transit or data-at-rest; thus completing the so-called data-security triad (Fig. 1).

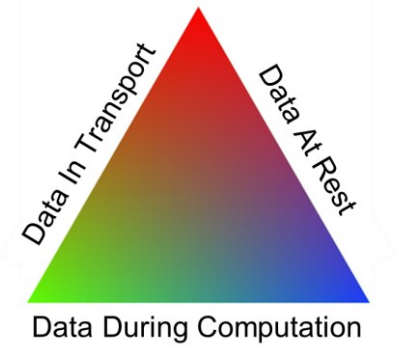

Figure 1. Data Security Triad

In 2008 a paper [1], by Lindell, Pinkas and Smart (as part of an EU FP7-ICT grant [a]) provided the first demonstration that actively secure (a.k.a. maliciously secure) MPC was possible [1]. Active security is the gold standard of security in this area, and until this paper no implementation had ever been presented of such a protocol. The paper implemented a prior protocol of Lindell and Pinkas, and computed a "toy example" of a comparison of two 16 bit numbers, which at the time took a few minutes to evaluate; today this operation is six orders of magnitude faster due to the large number of works which this paper inspired. The subsequent improvements are such that almost all commercial products in this space now utilize actively secure protocols.

Smart extended this work in the following year [2], performing the first large secure computation, namely the evaluation of the Advanced Encryption Standard (AES) circuit (funded by EU FP7-ICT project CACE [a]). This paper established this problem as the key performance metric in this area, an approach subsequently used in a large number of follow

up papers. The calculation initially took 19 minutes, a time which in subsequent papers has been drastically reduced to just a few milliseconds. The paper [2] introduces a number of performance optimizations still in use today. This idea of evaluating AES via MPC led subsequently to the forming of Unbound Tech by Smart and others.

Further funding from the EU [b,c], EPSRC [d] and DARPA [e] enabled investigation into the case of protocols for more than two parties. This led to the development in 2011 of the so-called SPDZ (Smart-Pedro-Damgard-Zakarias; pronounced "Speedz") protocol [3]. The SPDZ protocol is today the most efficient general-purpose protocol for MPC in the case of dishonest majority for a large number of parties. The protocol was extended in various works, e.g. [4], and it is this later version which now forms the basis of the SCALE-MAMBA open-source software suite [E]. SCALE-MAMBA was started in Bristol and has since transferred to KU Leuven. The software is available as an open source library, and its development has been funded by DARPA, ERC, EPSRC, FWO, IARPA and the Royal Society. Variants of the software are used by companies, including Cosmian and Galois, who have also provided development support.

The SPDZ protocol is only practical due to the extensive use it makes of the so-called Smart-Vercauteren packing technique for homomorphic encryption, which was initiated in the paper [5], and then extensively exploited and developed in [6]. The initial paper [5] (funded by the EU [b]) provided the first implementation and introduced the idea of Single Instruction Multiple Data (SIMD) operations on FHE ciphertexts. This technique enables massively parallel homomorphic operations to be carried out. By performing many operations in parallel one can obtain very high throughput, and hence one mitigates against the high latency inherent in using homomorphic encryption. The paper [5] (along with Gentry's Thesis) led directly to the PROCEED programme of DARPA [e] which was a USD30 million program to develop MPC and FHE applications. The PROCEED programme led to many of the performance improvements which have resulted in this technology moving into the mainstream, such as paper [6]. The paper [6] (funded by [b,d,e] as well as an ERC Advanced grant awarded to Smart [c]) did for FHE what paper [2] did for MPC, and established a number of optimizations and performance improvements which turned FHE from a theoretical endeavour into one which could perform useful functions.

This push to turn the theory of secure computation into reality has been led internationally by Smart, leading to an invitation to give the Invited Talk at EuroCrypt 2017 in Paris (the premier cryptography conference in Europe), as well as invitations to discuss the work at Google and Microsoft's headquarters, as well the award of a second ERC Advanced Grant of EUR2,499,938 (ERC-2015-AdG-690978-IMPaCT) in 2015.

3. References to the research

[1] Lindell Y, Pinkas B, **Smart NP**. (2008). Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries. *Security and Cryptography for Networks,* 5229, 2-20. DOI:10.1007/978-3-540-85855-3_2

[2] Pinkas B, Schneider T, **Smart NP**, Williams SC. (2009). Secure Two-Party Computation Is Practical. *Advances in Cryptology,* 5912, 250-267. DOI:10.1007/978-3-642-10366-7_15

[3] Damgård I, Pastro V, **Smart NP**, Zakarias S. (2012). Multiparty Computation from Somewhat Homomorphic Encryption. *Advances in Cryptology*, 7417, 643-662. DOI:10.1007/978-3-642-32009-5_38

[4] Damgård I, Keller M, Larraia E, Pastro V, Scholl P, **Smart NP**. (2013). Practical Covertly Secure MPC for Dishonest Majority - Or: Breaking the SPDZ Limits. *Computer Security,* 8134, 1-18. DOI:10.1007/978-3-642-40203-6_1

[5] **Smart NP**, Frederik Vercauteren F (2010). Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. *Public Key Cryptography,* 6056, 420-443. DOI:10.1007/978-3-642-13013-7_25

[6] Gentry C, Halevi S, **Smart NP.** (2012). Fully Homomorphic Encryption with Polylog Overhead, *Advances in Cryptology,* 7237, 465-482. DOI:10.1007/978-3-642-29011-4_28

Relevant Grants:

a) **Smart NP**. Computer Aided Cryptography Engineering (CACE), EU FP7-ICT, 2008 - 2010, GBP397,766 (Bristol portion)

b) **Smart NP**. European Network of Excellence in Cryptography – Phase II (ECRYPT II), EU FP7-ICT, 2008 – 2013, GBP127,723 (Bristol portion)

c) **Smart NP.** CRIPTO: Cryptography Research Involving Practical and Theoretical Outlooks, EU FP7-IDEAS-ERC, 2011 – 2016, EUR2,102,041

d) **Smart NP.** COED: Computing on Encrypted Data, EPSRC, 2011 – 2015, GBP970,000

e) **Smart NP**. PROgramming Computation on EncryptEd Data (PROCEED), DARPA, USD433,845 (Bristol portion)

f) **Smart NP**. Brandeis, DARPA, USD883,126 (Bristol portion)

4. Details of the impact

Commercialisation of new technology and company growth

The development of MPC as a practical technology, and the techniques developed in the above research, have addressed the fundamental issue of unlocking data without compromising user privacy, which until this point had inhibited growth in secure computation innovation. Indeed, Gartner (the major provider of analysis to companies re market trends) now lists MPC as an explicit technology on the "upward" curve of its yearly technology hype-cycles in at least five technology areas in each of the last three years[1]. MPC and FHE are now being employed by numerous organisations as a way to unlock the value in data without compromising user privacy, an ecosystem of economic activity only possible as a direct result of the work of Smart. Start-ups and SMEs utilising MPC and FHE have now generated well over USD100 million in venture capital investment. These include:

- **Unbound Tech**, founded in 2014 by Smart and Lindell (Bar-Ilan University). Unbound utilises the developments in the technology outlined in [1] and [2] to secure cryptographic keys. The company has received over USD40 million in investment from Innovation Endeavours, Citi Ventures, Evolution Equity Partners, Goldman Sachs and BlueRed Partners [A] and is also the recipient of an EU SME Instrument award. The company has grown to over 50 employees based across three continents [A]. It markets products in a number of vertical markets, including cryptocurrency exchange, code signing solutions and Google Cloud services [A]. In 2019, Unbound was named as a "cool vendor" by Gartner [A] and their main product has been certified by the US standard agency NIST (National Institute of Standards and Technology) to FIPS 140 Level 2 (Federal Information Processing Standard). It is the first MPC enabled product to be certified in this way [A].

- **Cybernetica** (a long-established SME from Estonia) market a product called Sharemind, which produces a "shared encrypted" database. A number of the techniques behind Sharemind derive from work conducted in Bristol on the SPDZ protocol [3] [Bi].

- **Duality**, established 2016, has attracted USD16 million Series A investment and grown to employ 26 people [Bii]. Leveraging FHE has enabled Duality to develop and deliver privacy-protecting computing to regulated data-industries and establish the primary open-source library for homomorphic encryption used in industry. Duality recognize the work of Smart, in particular [5] and [6], on making their usage of FHE practical [Bii].

[1] https://www.gartner.com/en/documents/3953753/hype-cycle-for-data-security-2019

- **Enveil**, founded 2016 after spinning out from the NSA, has raised USD15 million from investors and used FHE to develop Trusted Compute in Untrusted Locations, allowing organisations to securely derive insights, cross-match, and search third-party data assets without compromising the security or ownership of the underlying data. Enveil, to whom Smart is an advisor, is also the first company marketing secure computing technologies which has had its offering certified to Common Criteria specifications. Enveil also recognizes the work of Smart, [5] and [6], on making their usage of FHE practical [Biii].

- **Partisia**, created in 2008, utilise MPC to enable efficient auction implementations for commodities where there is no trusted auctioneer, and buy/sell orders need to be kept secret. It has been able to use MPC to progress from their initial focus on secure auctions to diversify into cryptographic key management and privacy-preserving statistics. Partisia utilises many of the ideas and protocols within the SPDZ family of protocols. Indeed, SPDZ was co-developed with researchers from Aarhus University, who are founders of both Partisia and Sepior [Biv].

- **Sepior**, founded in 2014, has used the SPDZ protocol to develop cryptographic keys in cloud web for companies in both APAC and the US, consequently leading to further financing through Horizon 2020 and SME Instrument Grants from the European Union. Both Partisia and Sepior recognize the influence of papers [3] and [4] on their products ([Biv and Bv]).

Furthermore, these organisations have come together to form the MPC Alliance [C], a consortium of over 30 companies (mainly small companies, but including some large companies such as Alibaba, Salesforce and Samsung). There is also the equivalent organisation, the HE Standards Forum, supporting the FHE companies in this space (including Alibaba, IBM, Intel, Microsoft, Samsung, and SAP) to foster public debate and encourage best practice in the security and privacy of personal data, advocating the use of MPC [C].

Informing technology standards in the US

NIST – the main US standards body, which accredits testing labs for the internationally influential Federal Information Processing Standards (FIPS) validation standards – are also interested in MPC as a mechanism to enable efficient testing of high value cryptographic products in certified testing laboratories. Some of the work resulting from SPDZ [3], such as the recent CAPA proposal (Smart CRYPTO 2018), is currently being investigated by NIST as a way of enabling such efficient testing. NIST organized a workshop [D] in early 2019 as a forerunner to standardization in this area and the related area of threshold cryptography (the key area of Unbound Tech). At the event NIST recognized that a major contributor to their interest in this area was a letter they received from various companies, which had been coordinated by Smart.

Public Policy Impacts

Concerns over the privacy of citizens has constrained exploitation of the power offered by data to inform policy-making and governmental delivery. Galois, a company of 130 employees, has been able to secure USD34 million in US Government funding by integrating the open-source SCALE-MAMBA [E] software, based on the SPDZ protocol [3, 4], into the Jana secure database under funding from the DARPA Brandeis programme [Fi]. DARPA alone has invested around USD200 million in technology programmes related to FHE and MPC since 2009 [Fii].

This has allowed Galois to collaborate with the US Government in the public policy field by developing technology transition prototypes for international coalitions for disaster relief, e.g. by enabling nation states to share sensitive data of their naval capacities to enable rescue and supply operations; by enabling sharing and analysis of sensitive network data for research in malware and cyber-attack detection; and by demonstrating how MPC technology makes practical the micro-economic analysis of trade information for the US Census Bureau.

These advances by Smart and Galois have stimulated policy debate in this area, with Galois and Smart providing evidence to the team of US Senator Wyden in the US. Senator Wyden has since led the call for MPC to be used to enable “evidenced based policy”, in areas where the evidence

may have privacy issues associated with it [H]. This resulted in two acts of Congress mentioning MPC (The "Right To Know Before You Go Act" of 2017, 2018 and the "Forward Act" of 2018 (H.R. 4479 and H.R. 6562)) [H].

The joint work of Cybernetica, Galois and Smart ([Bi] and [Fi]) has led to a report on the technology for a United Nations working group on processing private data; work which the team leader has said was "greatly influenced" by the University of Bristol's work in this space [I].

5. Sources to corroborate the impact

[A] Unbound Tech (2020). Corroborating Statement, CEO (Attached: PR Newswire and company case studies)

[B] Corroborating statements from companies commercialising MPC technology, including: i) Cybernetica (2020), Member of management board; ii) Duality (2020), CTO; iii) Enveil (2020), CEO and Press Release (Enveil Achieves NIAP Common Criteria Certification); iv) Partisia (2020), CEO; v) Sepior (2020), CTO.

[C] Organisations supporting MPC/FHE, including: i) MPC Alliance, GlobalNewswire (2019). Industry Leaders Launch MPC Alliance to Elevate Security and Privacy of Online Services and ii) Homomorphic Encryption Standardization (2017-2020), https://homomorphicencryption.org/; [Accessed 15 May 2020].

[D] NIST workshops i) NIST (2019). NIST Threshold Cryptography Workshop 2019 and ii) NIST (2020). NIST Workshop on Multi-Party Threshold Schemes 2020 [Accessed 27 Oct 2020].

[E] SCALE-MAMBA Open source library, https://homes.esat.kuleuven.be/~nsmart/SCALE/, [Accessed 27 Oct 2020].

[F] Corroborating statements from the DARPA Brandeis programme, including: i) Galois Inc (2020), Principal Scientist; and ii) DARPA (2020), Programme Manager

[G] Senator Wyden (2017). Open Letter on Privacy Techniques [Accessed 15 May 2020].

[H] Acts of Congress, including: Forward Act of 2018, H.R. 6562, 115th Congress, 2nd Session (2018) and The Student Right to Know Before you Go Act of 2017, H.R. 4479, 115th Congress 1st Session (2019)

[I] United Nations working group on data privacy, i) UN (2020). Supporting Letter - Chair of UN Privacy Preserving Techniques Task Team; and ii) UN (2019) Handbook on Privacy-Preserving Computation Techniques [Accessed 28 July 2020]