Kisaco Research

Kisaco Innovation Radar Pioneer 2021

Kisaco Innovation Radar on Secure and Private Compute 2021

Motivation, Contents Table, list of Figures, and example content

Publication Date: 1 Feb 2021. Product code KR370.1

Michael Azoff

Motivation

The cybersecurity landscape is undergoing radical transformation through breakthrough technologies that for the first time offer secure and private compute (SPC) to enterprises. We wish to encrypt data across the three phases that track its complete lifecycle: at rest, in flight, and during compute. With encryption of data throughout its lifecycle and with the encryption keys held by and never leaving the data owner, it is possible to offer maximum security and privacy. The challenge has been creating viable encryption in compute schemes – this is what SPC technologies tackle. The usual, current practice in any computation on encrypted data is that first you need to decrypt it, perform the required computation, and then encrypt the results. The challenge and 'holy grail' has been to compute with encrypted data and do so within reasonable time and cost.

SPC has emerged in recent years with a number of competing technologies which each have their strengths and weaknesses. This report explains the technology and market landscape and profiles some of the new leading players pioneering this field. We cover technologies such as homomorphic encryption (HE) and its various modes, including fully homomorphic encryption (FHE), as well as enclaves in trusted execution environments (TEE) and applications in secure multi-party computation (MPC). We also name the key organizations that are driving this community, describe the efforts in standardization, and identify business use cases that enterprises should be aware and learn about today. The report further provides profiles on vendors at the cutting edge of SPC: Cornami, Cybernetica, Decentriq, Duality, Inpher, and Zama.

What you will learn:

- How is secure and private compute (SPC) different from other forms of data encryption and what will its impact be on businesses and how we use the internet and cloud.
- What are the key technologies enabling SPC, including an introduction to FHE, TEE and MPC.
- The strengths and weaknesses of the key enabling technologies.
- What is on the roadmap in SPC and what will be the impact of hardware accelerators.
- Which are the key SPC vendor associations and what is their activities.
- We provide in-depth profiles on each participating vendor, who are pioneers in SPC.

Contents

© Kisaco Research. All rights reserved. Unauthorized reproduction prohibited.

Figures (including tables)

© Kisaco Research. All rights reserved. Unauthorized reproduction prohibited.

Example Content

Introduction to SPC

Naming conventions and associations

SPC is our choice of label for cryptographic technology applied to the compute part of the data lifecycle. However, cryptographic communities are using labels such as privacy-preserving computing, and data oblivious computing. Furthermore, three associations have formed which also embrace certain choices of terminology, and we identify these as follows:

- **Confidential Computing Consortium**: This vendor consortium uses the preferred term “confidential computing” to refer to TEE available on CPU hardware.
- **Homomorphic Encryption Standardization**: This organization spans vendors, government and academia and, as the name implies, is concerned with HE.
- **MPC Alliance**: This is a vendor consortium that is concerned with MPC. MPC is a task or requirement and needs to be specified with the cryptographic technology being applied. In many cases the choice is secret sharing, and it appears there is reluctance with some vendors that use HE or TEE to use the term MPC when the use case is MPC. In this report we qualify the label MPC with the technology used.

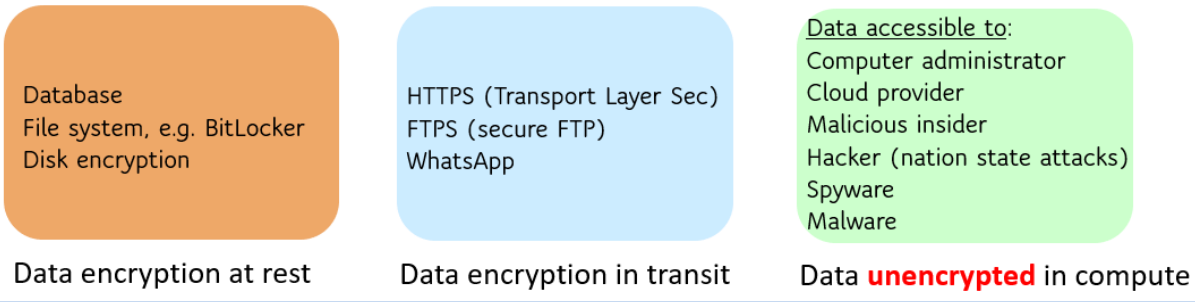
© Kisaco Research. All rights reserved. Unauthorized reproduction prohibited.

The appendix provides further details on these vendor and community associations.

What is new and possible today that is different from the past

Thinking about the journey that data takes in typical scenarios: it is generated and protected in storage by encryption; it is transferred across networks between computers such as sending to the cloud and protected during transit by encryption. Traditionally the data is then decrypted in order that computation can be performed on the data, such as feeding it to a neural network for training or performing some statistical analysis on the data. What SPC offers is protection of the data during computation. This means there is no access to the data at any point during its compute without protection, the only people able to retrieve the plaintext (the readable message or data) are the owners of the encryption keys. This applies even to staff administering the computers in which the computation occurs – traditionally administrators could observe private data if they wished and with SPC this is not possible. To summarize what is new: data can now be protected throughout its lifecycle: during storage, in transit, and the new part, during compute – see Figure 1.

Figure 1: Securing the data lifecycle: the problem without encrypting compute



Source: Kisaco Research

There are several SPC technologies in play today and new ones are emerging from academia, a new generation of startups are emerging to bring these technologies into general use across enterprises and even consumers. We witness how secure hypertext transfer protocol (https) is now a default in the web over the insecure http standard, similarly we expect SPC technologies to become ubiquitous and in some applications to be compulsory. This will happen as standards are created and adopted, and as awareness and education of SPC grows.

Vendor analysis

Kisaco Research received briefings from leading players in the SPC space. The participating vendors are listed in Figure 8 and are profiled in this section. The table summaries key technologies available from the vendor and the FHE libraries used where relevant. All the vendors' primary business is offering software cryptographic solutions except Cornami which is developing a FHE chip accelerator. The software vendors are also partnering with hardware accelerator providers of GPU, FPGA, and ASIC.

© Kisaco Research. All rights reserved. Unauthorized reproduction prohibited.

Figure 8: The vendors profiled in this report and key technologies they offer

Vendor	FHE	FHE library	MPC	TEE
Cornami (acceleration chip)	✓	Any		
Cybernetica			✓	
Decentriq				✓
Duality	✓	Palisade		
Inpher	✓	TFHE	✓	
Zama	✓	Concrete (TFHE)		

Source: Kisaco Research

Author

Michael Azoff, Chief Analyst

michael.azoff@kisacoresearch.com

Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Kisaco Research Ltd. our affiliates or other third-party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Kisaco Research Ltd. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Kisaco Research Ltd.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Kisaco Research Ltd. nor any person engaged or employed by Kisaco Research Ltd. accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard - readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Kisaco Research Ltd.

CONTACT US

www.kisacoresearch.com
Michael.azoff@kisacoresearch.com

© Kisaco Research. All rights reserved. Unauthorized reproduction prohibited.