

IEEE Recommended Practice for Secure Multi-Party Computation

IEEE Computer Society

Developed by the
Standards Activities Board Committee

IEEE Std 2842™-2021

IEEE Recommended Practice for Secure Multi-Party Computation

Developed by the

Standards Activities Board Committee
of the
IEEE Computer Society

Approved 23 September 2021

IEEE SA Standards Board

Abstract: Data has become one of the most important assets in ICT area. Secure multi-party computation plays a very important role in balancing data usage and data protection. It could build trust and security in data collaboration and big data analysis related areas. A technical framework for secure multi-party computation is provided in this standard, including specifying the following: an overview of secure multi-party computation; a technical framework of secure multi-party computation; security levels of secure multi-party computation; and use cases based on secure multi-party computation.

Keywords: IEEE 2842™, MPC, secure multi-party computation, technical framework

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2021 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 5 November 2021. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-7986-8 STD24960
Print: ISBN 978-1-5044-7987-5 STDPD24960

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

This is a preview. Click here to purchase the full publication.