

Grant Agreement Number: 825225

Safe-DEED

www.safe-deed.eu

**Implementation of Cryptographic Building Blocks and
Specialized Protocols v1/3**

Deliverable number	<i>D5.5</i>
Dissemination level	<i>Public</i>
Delivery data	<i>due 29.11.2019</i>
Status	<i>Final</i>
Authors	<i>Lukas Helminger, Fabian Schmid, Roman Walch</i>



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825225.

Executive Summary

In this deliverable, we describe the implementation of a new cryptographic primitive called multi-party public-key accumulator (MPC-accumulator), which was developed in the Safe-DEED project. An MPC-accumulator is a basic building block for privacy-enhanced technology. This document should enable security experts and software engineers to use MPC-accumulators in their applications. We fully describe the functionality of MPC-accumulators and their possible applications in deliverable D5.3. Since the theoretical description of a cryptographic primitive alone is not enough to get wide acceptance by the community we implemented MPC-accumulators using an open-source MPC-framework.

The implementation uses advanced cryptographic primitives like elliptic curve cryptography and secret sharing. Therefore, we are not only providing the source code but comprehensive documentation of the code. In addition, we give easy to follow instructions on how to download, install, and edit the provided source code of MPC-accumulators.

Table of Contents

- 1 Introduction** **3**
- 1.1 Dependencies 3
- 1.1.1 FRESCO 3
- 1.1.2 IAIK ECCelerate 3
- 2 The Build Process** **3**
- 3 The Program Structure** **4**
- 4 Conclusion** **5**
- 5 References** **6**
- A API** **6**

1 Introduction

In deliverable D5.3, we developed a new cryptographic primitive called multi-party public-key accumulators (MPC-accumulators). To make MPC-accumulators available to the community, we also implemented them with an open-source MPC-framework. Since we choose to use elliptic curves as a building block, we are talking about elliptic curve accumulators. This deliverable aims to provide a quick overview on how to download, install, and edit the provided source code of the elliptic curve accumulator running with Secure Multi-Party Computation. The code is written in Java and licensed under the open-source MIT license¹. This document is organized as follows.

First, there will be a short description of the dependencies. Secondly, in Section 2, we will look at a guide on how to build and run the demonstration. Then there will be an elaboration of the program structure (Section 3), the changes made to FRESCO [1], and the location of the code of this contribution. In the end, we provide the full API of our elliptic curve accumulator (Section A).

1.1 Dependencies

1.1.1 FRESCO

For the proof-of-concept implementation of our protocols, we used FRESCO. We chose FRESCO because it allows fast prototyping of MPC protocols, is open-source, and has an active developer community. Since we needed to adapt the SPDZ protocol [3, 2] to be able to run elliptic curve operations, we made a lot of changes to the framework. Thus we provide an altered version of FRESCO ourselves, where we omitted parts we do not need and added our changed files.

1.1.2 IAIK ECCelerate

Our implementation combines Secure Multi-Party Computation with elliptic curve cryptography. As mentioned above, we rely on FRESCO for our MPC computations. For the elliptic curve calculations, we used the IAIK ECCelerate library [4] and the Java Cryptography Extension (JCE), previously developed by our team at the TU Graz. It is, therefore, necessary to get a license of the ECCelerate, to run our demonstration. For research purposes, there exists educational license². There is also an ECCelerate add-on, this includes speedups for the ECC computations. The curves used by the add-on may be patented in certain countries. When it is ensured that these curves may be used, one can integrate the add-on as well.

2 The Build Process

The project is developed using maven³. When using maven as a build manager, one has to install the ECCelerate .jar file in the local maven repository using the following command.

¹<https://mit-license.org/>

²<https://jce.iaik.tugraz.at/sic/Sales/Licences/Educational>

³<https://maven.apache.org/>

```
mvn install:install-file -Dfile=<path-to-file> -DgroupId=<group-id> -DartifactId=<artifact-id> -Dversion=<version> -Dpackaging=<packaging>
```

- <path-to-file> has to specify the path to the .jar file (the java archive)
- <group-id> has to specify the group, in our case iaik.
- <artifact-id> the name under which the artifact will be installed: iaik_eccelerate for the ECC library.
- <version> This demonstrator was developed and tested under version 6.0.
- <packaging> When following the instruction above one has to specify the packaging as jar.

Note that the demonstrator also depends on a JCE library, developed at IAIK. If one wants to run the program without this dependency, remove it from the `suite/spdz/pom.xml` and make sure to provide a different JCE framework. The ECCelerate add-on is an optional improvement to the ECC library. This add-on can be installed as described above. After installing it to the local maven repository, it has to be added as a dependency in the `suite/spdz/pom.xml` file.

Following the previous steps, one has installed the ECCelerate library in the local maven repository. Now the build process can be started. Navigate to the `demos/MPC-ACC` directory to find the Makefile for this demonstrator. There are several make targets. To make a full and clean installation, execute the command `make build`. This command will install FRESCO, the ECC library, and the demonstrator. Then the assembled jar file will be put in a specific folder so that the run target will find it later.

3 The Program Structure

The implementation of the demonstrator is embedded in the demo folder of FRESCO. We needed to adapt FRESCO to our needs in terms of elliptic curve operations. However, we kept the maven directory structure.

Core: The Core folder holds the foundation of the FRESCO framework. The general layout and fundamental definitions are given there. In there, we merely added some output functions to the Socket Network class. These output functions were needed to perform benchmarking.

Suite: FRESCO implements multiple MPC protocols. These protocols are found in the suite directory. For our demonstration, we needed the SPDZ protocol suite, since it provides security against malicious adversaries and allows more than two parties to participate in the protocol. For compactness, we omitted the other protocol suites from code. The dependencies of our adaptations can be found in the `pom.xml` file of SPDZ. Our Adaptations themselves are located in the `ECCExtensions` directory in the SPDZ implementation.

Tools: Tools contains various protocols needed by the protocol suites. The mascot protocol and oblivious transfer protocol can be found here. The mascot protocol had to be adapted to the changes made in the SPDZ implementation.

Demos: Here in the `MPC-ACC` directory, the actual MPC elliptic curve accumulator is positioned. When the project is successfully built, the project can be run by the provided execution scripts. As a starting point, one might look at the `make run` target. Then one could look into the scripts facilitating execution in a distributed environment.

For further information on the algorithm, the design choices, and the structure, we provide the full API (Section A) below. In addition, the source code⁴ can be found online as soon as the submission process of the corresponding paper is finished.

4 Conclusion

In this deliverable, we looked at the concrete implementation of MPC-accumulators - a cryptographic primitive developed in the context of Safe-DEED. MPC-accumulators show how one can gain performance through distributed trust. Our goal is that the community can easily use MPC-accumulators. Therefore we included a step-by-step explanation of the build process (Section 2). For a complete understanding, we explained the program structure (Section 3) and put a lot of effort into describing the API of the MPC-accumulators. For the next version of this deliverable, we plan to build privacy-friendly real-world applications. These real-world applications will be based on the most recent cryptographic primitives, like MPC-accumulators. In addition, we always try to make our applications accessible to a broad audience. To achieve this, we are currently investigating how to integrate our solutions into big open-source software projects.

⁴<https://github.com/orgs/Safe-DEED/dashboard>

5 References

- [1] Alexandra Institute. FRESCO - a FRamework for Efficient Secure Computation. <https://github.com/aicis/fresco/>, 2019.
- [2] Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P. Smart. Practical covertly secure MPC for dishonest majority - or: Breaking the SPDZ limits. In *ESORICS*, volume 8134 of *LNCS*, pages 1–18. Springer, 2013.
- [3] Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In *CRYPTO*, volume 7417 of *LNCS*, pages 643–662. Springer, 2012.
- [4] Christian Hanser and Sebastian Ramacher. IAIK ECCelerate, 2019. URL: https://jce.iaik.tugraz.at/sic/Products/Core_Crypto_Toolkits/ECCelerate.

A API

MPC-Accumulator

Generated by Doxygen 1.8.13

Contents

1 Namespace Index	1
1.1 Packages	1
2 Hierarchical Index	2
2.1 Class Hierarchy	2
3 Class Index	3
3.1 Class List	3
4 File Index	5
4.1 File List	5
5 Namespace Documentation	6
5.1 Package at	6
5.2 Package at.iaik	6
5.3 Package at.iaik.mpc_acc	6
5.4 Package at.iaik.utils	7
5.5 Package dk	7
5.6 Package dk.alexandra	7
5.7 Package dk.alexandra.fresco	7
5.8 Package dk.alexandra.fresco.suite	7
5.9 Package dk.alexandra.fresco.suite.spdz	7
5.10 Package dk.alexandra.fresco.suite.spdz.ECCEExtension	8

CONTENTS	ii
6 Class Documentation	8
6.1 at.iaik.mpc_acc.Accumulator Class Reference	8
6.1.1 Detailed Description	9
6.1.2 Constructor & Destructor Documentation	9
6.1.3 Member Function Documentation	9
6.1.4 Member Data Documentation	13
6.2 at.iaik.mpc_acc.AccumulatorDemo Class Reference	14
6.2.1 Detailed Description	15
6.2.2 Constructor & Destructor Documentation	15
6.2.3 Member Function Documentation	16
6.2.4 Member Data Documentation	19
6.3 at.iaik.mpc_acc.Auxillary Class Reference	20
6.3.1 Detailed Description	21
6.3.2 Constructor & Destructor Documentation	21
6.3.3 Member Function Documentation	22
6.3.4 Member Data Documentation	23
6.4 at.iaik.utils.CmdLineParser.BuilderParams Class Reference	24
6.4.1 Detailed Description	24
6.4.2 Constructor & Destructor Documentation	25
6.4.3 Member Function Documentation	25
6.4.4 Member Data Documentation	26
6.5 at.iaik.utils.CmdLineParser Class Reference	27
6.5.1 Detailed Description	28
6.5.2 Member Function Documentation	28
6.5.3 Member Data Documentation	29
6.6 at.iaik.mpc_acc.EvalResult Class Reference	31
6.6.1 Detailed Description	31
6.6.2 Constructor & Destructor Documentation	31
6.6.3 Member Function Documentation	33
6.6.4 Member Data Documentation	33

6.7	at.iaik.mpc_acc.Main Class Reference	33
6.7.1	Detailed Description	34
6.7.2	Member Function Documentation	34
6.7.3	Member Data Documentation	35
6.8	at.iaik.mpc_acc.MerkleTree Class Reference	35
6.8.1	Detailed Description	36
6.8.2	Constructor & Destructor Documentation	36
6.8.3	Member Function Documentation	37
6.8.4	Member Data Documentation	38
6.9	at.iaik.mpc_acc.MPC_Acc Class Reference	39
6.9.1	Detailed Description	39
6.9.2	Constructor & Destructor Documentation	40
6.9.3	Member Function Documentation	40
6.9.4	Member Data Documentation	43
6.10	at.iaik.mpc_acc.MPC_Add Class Reference	45
6.10.1	Detailed Description	46
6.10.2	Constructor & Destructor Documentation	46
6.10.3	Member Function Documentation	46
6.10.4	Member Data Documentation	46
6.11	at.iaik.mpc_acc.MPC_Del Class Reference	47
6.11.1	Detailed Description	48
6.11.2	Constructor & Destructor Documentation	48
6.11.3	Member Function Documentation	48
6.11.4	Member Data Documentation	49
6.12	at.iaik.mpc_acc.MPC_Eval Class Reference	49
6.12.1	Detailed Description	50
6.12.2	Constructor & Destructor Documentation	50
6.12.3	Member Function Documentation	51
6.12.4	Member Data Documentation	51
6.13	at.iaik.mpc_acc.MPC_Gen Class Reference	52

CONTENTS	iv
6.13.1 Detailed Description	52
6.13.2 Constructor & Destructor Documentation	53
6.13.3 Member Function Documentation	53
6.13.4 Member Data Documentation	53
6.14 at.iaik.mpc_acc.MPC_TripleDummy Class Reference	54
6.14.1 Detailed Description	54
6.14.2 Member Function Documentation	54
6.14.3 Member Data Documentation	55
6.15 at.iaik.mpc_acc.MPC_WitCreate Class Reference	56
6.15.1 Detailed Description	57
6.15.2 Constructor & Destructor Documentation	57
6.15.3 Member Function Documentation	57
6.15.4 Member Data Documentation	57
6.16 at.iaik.mpc_acc.MPC_WitUpdateAdd Class Reference	58
6.16.1 Detailed Description	59
6.16.2 Constructor & Destructor Documentation	59
6.16.3 Member Function Documentation	59
6.16.4 Member Data Documentation	60
6.17 at.iaik.mpc_acc.MPC_WitUpdateDel Class Reference	60
6.17.1 Detailed Description	61
6.17.2 Constructor & Destructor Documentation	61
6.17.3 Member Function Documentation	61
6.17.4 Member Data Documentation	62
6.18 at.iaik.utils.MPCBuilder< ObjectT > Class Template Reference	62
6.18.1 Detailed Description	64
6.18.2 Constructor & Destructor Documentation	64
6.18.3 Member Function Documentation	64
6.18.4 Member Data Documentation	68
6.19 at.iaik.mpc_acc.MPCParams Class Reference	70
6.19.1 Detailed Description	70

CONTENTS	v
6.19.2 Member Function Documentation	71
6.20 at.iaik.mpc_acc.MPCParamsBuilder Class Reference	72
6.20.1 Detailed Description	73
6.20.2 Constructor & Destructor Documentation	73
6.20.3 Member Function Documentation	73
6.21 at.iaik.utils.NetworkLoggingDecorator Class Reference	74
6.21.1 Detailed Description	75
6.21.2 Constructor & Destructor Documentation	75
6.21.3 Member Function Documentation	75
6.21.4 Member Data Documentation	76
6.22 at.iaik.utils.NetworkManager Class Reference	77
6.22.1 Detailed Description	79
6.22.2 Constructor & Destructor Documentation	79
6.22.3 Member Function Documentation	79
6.22.4 Member Data Documentation	81
6.23 at.iaik.mpc_acc.Node Class Reference	83
6.23.1 Detailed Description	83
6.23.2 Constructor & Destructor Documentation	83
6.23.3 Member Function Documentation	84
6.23.4 Member Data Documentation	84
6.24 at.iaik.utils.NetworkLoggingDecorator.PartyStats Class Reference	85
6.24.1 Detailed Description	85
6.24.2 Member Function Documentation	85
6.24.3 Member Data Documentation	86
6.25 at.iaik.mpc_acc.Polynomial Class Reference	86
6.25.1 Detailed Description	87
6.25.2 Constructor & Destructor Documentation	87
6.25.3 Member Function Documentation	87
6.25.4 Member Data Documentation	88
6.26 at.iaik.mpc_acc.MerkleTree.Position Enum Reference	89

Generated by Doxygen

CONTENTS	vi
6.26.1 Detailed Description	89
6.26.2 Member Data Documentation	89
6.27 at.iaik.mpc_acc.MerkleTree.ProofNode Class Reference	89
6.27.1 Constructor & Destructor Documentation	90
6.27.2 Member Data Documentation	90
6.28 dk.alexandra.fresco.suite.spdz.ECCEExtension.SECPoint Interface Reference	91
6.28.1 Detailed Description	91
6.29 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol Class Reference	92
6.29.1 Detailed Description	93
6.29.2 Constructor & Destructor Documentation	93
6.29.3 Member Function Documentation	93
6.29.4 Member Data Documentation	94
6.30 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps Class Reference	95
6.30.1 Detailed Description	96
6.30.2 Constructor & Destructor Documentation	96
6.30.3 Member Function Documentation	96
6.30.4 Member Data Documentation	99
6.31 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPoint Class Reference	99
6.31.1 Detailed Description	100
6.31.2 Constructor & Destructor Documentation	101
6.31.3 Member Function Documentation	101
6.31.4 Member Data Documentation	103
6.32 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol Class Reference	103
6.32.1 Detailed Description	104
6.32.2 Constructor & Destructor Documentation	104
6.32.3 Member Function Documentation	105
6.32.4 Member Data Documentation	105
6.33 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar Class Reference	106
6.33.1 Detailed Description	107
6.33.2 Constructor & Destructor Documentation	107

CONTENTS	vii
6.33.3 Member Function Documentation	107
6.33.4 Member Data Documentation	107
6.34 dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzMultECCProtocol Class Reference	108
6.34.1 Detailed Description	109
6.34.2 Constructor & Destructor Documentation	109
6.34.3 Member Function Documentation	109
6.34.4 Member Data Documentation	110
6.35 dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzOpenedValueECCStoreImpl Class Reference	110
6.35.1 Detailed Description	111
6.36 dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzOutputPointProtocol Class Reference	111
6.36.1 Detailed Description	112
6.36.2 Constructor & Destructor Documentation	112
6.36.3 Member Function Documentation	112
6.36.4 Member Data Documentation	113
6.37 at.iaik.mpc_acc.Witness Class Reference	113
6.37.1 Detailed Description	114
6.37.2 Constructor & Destructor Documentation	114
6.37.3 Member Function Documentation	114
6.37.4 Member Data Documentation	115
7 File Documentation	115
7.1 Accumulator.java File Reference	115
7.2 AccumulatorDemo.java File Reference	115
7.3 Auxillery.java File Reference	116
7.4 CmdLineParser.java File Reference	116
7.5 EvalResult.java File Reference	116
7.6 Main.java File Reference	116
7.7 MerkleTree.java File Reference	117
7.8 MPC_Acc.java File Reference	117
7.9 MPC_Add.java File Reference	117
7.10 MPC_Del.java File Reference	117

1	Namespace Index	1
<hr/>		
7.11	MPC_Eval.java File Reference	117
7.12	MPC_Gen.java File Reference	118
7.13	MPC_TripleDummy.java File Reference	118
7.14	MPC_WitCreate.java File Reference	118
7.15	MPC_WitUpdateAdd.java File Reference	118
7.16	MPC_WitUpdateDel.java File Reference	119
7.17	MPCBuilder.java File Reference	119
7.18	MPCParams.java File Reference	119
7.19	MPCParamsBuilder.java File Reference	119
7.20	NetworkLoggingDecorator.java File Reference	119
7.21	NetworkManager.java File Reference	120
7.22	Node.java File Reference	120
7.23	Polynomial.java File Reference	120
7.24	SECPPoint.java File Reference	120
7.25	SpdzECCMacCheckProtocol.java File Reference	121
7.26	SpdzECCOps.java File Reference	121
7.27	SpdzECPoint.java File Reference	121
7.28	SpdzKnownMultECCProtocol.java File Reference	121
7.29	SpdzKnownScalar.java File Reference	121
7.30	SpdzMultECCProtocol.java File Reference	122
7.31	SpdzOpenedValueECCStoreImpl.java File Reference	122
7.32	SpdzOutputPointProtocol.java File Reference	122
7.33	Witness.java File Reference	122
	Index	123

1 Namespace Index

1.1 Packages

Here are the packages with brief descriptions (if available):

[at](#) 6

2 Hierarchical Index	2
at.iaik	6
at.iaik.mpc_acc	6
at.iaik.utils	7
dk	7
dk.alexandra	7
dk.alexandra.fresco	7
dk.alexandra.fresco.suite	7
dk.alexandra.fresco.suite.spdz	7
dk.alexandra.fresco.suite.spdz.ECCEExtension	8

2 Hierarchical Index

2.1 Class Hierarchy

This inheritance list is sorted roughly, but not completely, alphabetically:

at.iaik.mpc_acc.Accumulator	8
at.iaik.mpc_acc.AccumulatorDemo	14
at.iaik.mpc_acc.Auxillery	20
at.iaik.utils.CmdLineParser.BuilderParams	24
at.iaik.utils.CmdLineParser	27
at.iaik.mpc_acc.EvalResult	31
at.iaik.mpc_acc.Main	33
at.iaik.mpc_acc.MerkleTree	35
at.iaik.mpc_acc.MPC_Acc	39
at.iaik.mpc_acc.MPC_TripleDummy	54
at.iaik.utils.MPCBuilder< ObjectT >	62
at.iaik.mpc_acc.MPCParamsBuilder	72
at.iaik.utils.MPCBuilder< MPCParams >	62
at.iaik.mpc_acc.MPCParams	70
at.iaik.mpc_acc.Node	83
at.iaik.utils.NetworkLoggingDecorator.PartyStats	85
at.iaik.mpc_acc.Polynomial	86
at.iaik.mpc_acc.MerkleTree.Position	89

Generated by Doxygen

3 Class Index	3
at.iaik.mpc_acc.MerkleTree.ProofNode	89
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps	95
at.iaik.mpc_acc.Witness	113
Application	
at.iaik.mpc_acc.MPC_Add	45
at.iaik.mpc_acc.MPC_Del	47
at.iaik.mpc_acc.MPC_Eval	49
at.iaik.mpc_acc.MPC_Gen	52
at.iaik.mpc_acc.MPC_WitCreate	56
at.iaik.mpc_acc.MPC_WitUpdateAdd	58
at.iaik.mpc_acc.MPC_WitUpdateDel	60
Closeable	
at.iaik.utils.NetworkLoggingDecorator	74
at.iaik.utils.NetworkManager	77
Computation	
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol	92
DRes	
dk.alexandra.fresco.suite.spdz.ECCEExtension.SECPoint	91
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPoint	99
Network	
at.iaik.utils.NetworkLoggingDecorator	74
OpenedValueStoreImpl	
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOpenedValueECCStoreImpl	110
PerformanceLogger	
at.iaik.utils.NetworkLoggingDecorator	74
Serializable	
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPoint	99
SpdzNativeProtocol	
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol	103
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar	106
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol	108
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOutputPointProtocol	111

3 Class Index

3.1 Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

Generated by Doxygen

3.1 Class List	4
at.iaik.mpc_acc.Accumulator	8
at.iaik.mpc_acc.AccumulatorDemo	14
at.iaik.mpc_acc.Auxillery	20
at.iaik.utils.CmdLineParser.BuilderParams	24
at.iaik.utils.CmdLineParser	27
at.iaik.mpc_acc.EvalResult	31
at.iaik.mpc_acc.Main	33
at.iaik.mpc_acc.MerkleTree	35
at.iaik.mpc_acc.MPC_Acc	39
at.iaik.mpc_acc.MPC_Add	45
at.iaik.mpc_acc.MPC_Del	47
at.iaik.mpc_acc.MPC_Eval	49
at.iaik.mpc_acc.MPC_Gen	52
at.iaik.mpc_acc.MPC_TripleDummy	54
at.iaik.mpc_acc.MPC_WitCreate	56
at.iaik.mpc_acc.MPC_WitUpdateAdd	58
at.iaik.mpc_acc.MPC_WitUpdateDel	60
at.iaik.utils.MPCBuilder< ObjectT >	62
at.iaik.mpc_acc.MPCParams	70
at.iaik.mpc_acc.MPCParamsBuilder	72
at.iaik.utils.NetworkLoggingDecorator	74
at.iaik.utils.NetworkManager	77
at.iaik.mpc_acc.Node	83
at.iaik.utils.NetworkLoggingDecorator.PartyStats	85
at.iaik.mpc_acc.Polynomial	86
at.iaik.mpc_acc.MerkleTree.Position	89
at.iaik.mpc_acc.MerkleTree.ProofNode	89
dk.alexandra.fresco.suite.spdz.ECCEExtension.SECPoint	91
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol	92
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps	95
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPoint	99
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol	103

4 File Index	5
dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzKnownScalar	106
dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzMultECCProtocol	108
dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzOpenedValueECCStoreImpl	110
dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzOutputPointProtocol	111
at.iaik.mpc_acc.Witness	113

4 File Index

4.1 File List

Here is a list of all files with brief descriptions:

Accumulator.java	115
AccumulatorDemo.java	115
Auxillery.java	116
CmdLineParser.java	116
EvalResult.java	116
Main.java	116
MerkleTree.java	117
MPC_Acc.java	117
MPC_Add.java	117
MPC_Del.java	117
MPC_Eval.java	117
MPC_Gen.java	118
MPC_TripleDummy.java	118
MPC_WitCreate.java	118
MPC_WitUpdateAdd.java	118
MPC_WitUpdateDel.java	119
MPCBuilder.java	119
MPCParams.java	119
MPCParamsBuilder.java	119
NetworkLoggingDecorator.java	119
NetworkManager.java	120
Node.java	120

Polynomial.java	120
SECPPoint.java	120
SpdzECCMacCheckProtocol.java	121
SpdzECCOps.java	121
SpdzECPPoint.java	121
SpdzKnownMultECCProtocol.java	121
SpdzKnownScalar.java	121
SpdzMultECCProtocol.java	122
SpdzOpenedValueECCStoreImpl.java	122
SpdzOutputPointProtocol.java	122
Witness.java	122

5 Namespace Documentation

5.1 Package at

Packages

- package [iaik](#)

5.2 Package at.iaik

Packages

- package [mpc_acc](#)
- package [utils](#)

5.3 Package at.iaik.mpc_acc

Classes

- class [Accumulator](#)
- class [AccumulatorDemo](#)
- class [Auxillery](#)
- class [EvalResult](#)
- class [Main](#)
- class [MerkleTree](#)
- class [MPC_Acc](#)
- class [MPC_Add](#)
- class [MPC_Del](#)
- class [MPC_Eval](#)
- class [MPC_Gen](#)

5.4 Package at.iaik.utils

7

- class [MPC_TripleDummy](#)
- class [MPC_WitCreate](#)
- class [MPC_WitUpdateAdd](#)
- class [MPC_WitUpdateDel](#)
- class [MPCParams](#)
- class [MPCParamsBuilder](#)
- class [Node](#)
- class [Polynomial](#)
- class [Witness](#)

5.4 Package at.iaik.utils

Classes

- class [CmdLineParser](#)
- class [MPCBuilder](#)
- class [NetworkLoggingDecorator](#)
- class [NetworkManager](#)

5.5 Package dk

Packages

- package [alexandra](#)

5.6 Package dk.alexandra

Packages

- package [fresco](#)

5.7 Package dk.alexandra.fresco

Packages

- package [suite](#)

5.8 Package dk.alexandra.fresco.suite

Packages

- package [spdz](#)

5.9 Package dk.alexandra.fresco.suite.spdz

Packages

- package [ECCEExtension](#)

Generated by Doxygen

5.10 Package dk.alexandra.fresco.suite.spdz.ECCEExtension

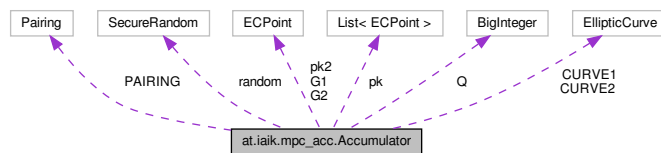
Classes

- interface [SECPPoint](#)
- class [SpdzECCMacCheckProtocol](#)
- class [SpdzECCOps](#)
- class [SpdzECPoint](#)
- class [SpdzKnownMultECCProtocol](#)
- class [SpdzKnownScalar](#)
- class [SpdzMultECCProtocol](#)
- class [SpdzOpenedValueECCStoreImpl](#)
- class [SpdzOutputPointProtocol](#)

6 Class Documentation

6.1 at.iaik.mpc_acc.Accumulator Class Reference

Collaboration diagram for at.iaik.mpc_acc.Accumulator:



Public Member Functions

- [Accumulator](#) (int size, int t)
- void [test](#) (List< BigInteger > X)
- BigInteger [getQ](#) ()

Private Member Functions

- BigInteger [getRandomScalar](#) ()
- void [Gen](#) ()
- [EvalResult Eval](#) (List< BigInteger > X, BigInteger r)
- [EvalResult Eval](#) (List< BigInteger > X)
- [Witness WitCreate](#) (ECPoint acc, [Auxillery](#) aux, BigInteger x)
- Boolean [Verify](#) (ECPoint acc, [Witness](#) wit, BigInteger x)
- [EvalResult Add](#) (ECPoint acc, [Auxillery](#) aux, BigInteger x)
- [EvalResult Delete](#) (ECPoint acc, [Auxillery](#) aux, BigInteger x)
- [Witness WitUpdate](#) ([Witness](#) wit, [Auxillery](#) aux, BigInteger x)

Private Attributes

- final Pairing [PAIRING](#)
- final EllipticCurve [CURVE1](#)
- final EllipticCurve [CURVE2](#)
- final BigInteger [Q](#)
- final ECPoint [G1](#)
- final ECPoint [G2](#)
- int [size](#)
- int [t](#)
- List< ECPoint > [pk](#)
- ECPoint [pk2](#)
- SecureRandom [random](#)

6.1.1 Detailed Description

A simple class computing the non-MPC, keyless accumulator.

Author

Roman Walch

6.1.2 Constructor & Destructor Documentation

6.1.2.1 Accumulator()

```
at.iaik.mpc_acc.Accumulator.Accumulator (
    int size,
    int t )
```

Constructor

Parameters

<i>size</i>	bitlength of the used pairing curves (400)
<i>t</i>	the threshold to precompute the public key

6.1.3 Member Function Documentation

6.1.3.1 Add()

```
EvalResult at.iaik.mpc_acc.Accumulator.Add (
    ECPoint acc,
    Auxillary aux,
    BigInteger x ) [private]
```

Adds an element to the accumulator

Parameters

<i>acc</i>	the accumulator
<i>aux</i>	the AUX data
<i>x</i>	the element

Returns

the new accumulator and AUX data

6.1.3.2 Delete()

```
EvalResult at.iaik.mpc_acc.Accumulator.Delete (  
    ECPPoint acc,  
    Auxillary aux,  
    BigInteger x ) [private]
```

Removes an element from the accumulator

Parameters

<i>acc</i>	the accumulator
<i>aux</i>	the AUX data
<i>x</i>	the element

Returns

the new accumulator and AUX data

6.1.3.3 Eval() [1/2]

```
EvalResult at.iaik.mpc_acc.Accumulator.Eval (  
    List< BigInteger > X,  
    BigInteger r ) [private]
```

Accumulates a set of elements into an accumulator

Parameters

<i>X</i>	the set of elements
<i>r</i>	a random element

Returns

the accumulator and the AUX data

6.1.3.4 Eval() [2/2]

```
EvalResult at.iaik.mpc_acc.Accumulator.Eval (  
    List< BigInteger > X ) [private]
```

Accumulates a set of elements into an accumulator

Parameters

X	the set of elements
---	---------------------

Returns

the accumulator and the AUX data

6.1.3.5 Gen()

```
void at.iaik.mpc_acc.Accumulator.Gen ( ) [private]
```

Generates the keys of the accumulator

6.1.3.6 getQ()

```
BigInteger at.iaik.mpc_acc.Accumulator.getQ ( )
```

6.1.3.7 getRandomScalar()

```
BigInteger at.iaik.mpc_acc.Accumulator.getRandomScalar ( ) [private]
```

Sample a random integer

Returns

a random integer

6.1.3.8 test()

```
void at.iaik.mpc_acc.Accumulator.test (  
    List< BigInteger > X )
```

A simple member to test the accumulator

Parameters

X	the set to be accumulated
---	---------------------------

Generated by Doxygen

6.1.3.9 Verify()

```
Boolean at.iaik.mpc_acc.Accumulator.Verify (  
    ECPint acc,  
    Witness wit,  
    BigInteger x ) [private]
```

Verifies if an element is part of the accumulator

Parameters

<i>acc</i>	the accumulator
<i>wit</i>	the witness to the element
<i>x</i>	the element

Returns

true if the element is part of the accumulator, false otherwise

6.1.3.10 WitCreate()

```
Witness at.iaik.mpc_acc.Accumulator.WitCreate (  
    ECPint acc,  
    Auxillary aux,  
    BigInteger x ) [private]
```

Creates a [Witness](#) to an element in the accumulator

Parameters

<i>acc</i>	the accumulator
<i>aux</i>	the AUX data
<i>x</i>	the element in the accumulator

Returns

the witness to the element

6.1.3.11 WitUpdate()

```
Witness at.iaik.mpc_acc.Accumulator.WitUpdate (  
    Witness wit,  
    Auxillary aux,  
    BigInteger x ) [private]
```

Updates a witness after element addition/removal

Parameters

<i>wit</i>	the previous witness of the element
<i>aux</i>	the AUX data
<i>x</i>	the element

Returns

the updated witness

6.1.4 Member Data Documentation

6.1.4.1 CURVE1

```
final EllipticCurve at.iaik.mpc_acc.Accumulator.CURVE1 [private]
```

6.1.4.2 CURVE2

```
final EllipticCurve at.iaik.mpc_acc.Accumulator.CURVE2 [private]
```

6.1.4.3 G1

```
final ECPoint at.iaik.mpc_acc.Accumulator.G1 [private]
```

6.1.4.4 G2

```
final ECPoint at.iaik.mpc_acc.Accumulator.G2 [private]
```

6.1.4.5 PAIRING

```
final Pairing at.iaik.mpc_acc.Accumulator.PAIRING [private]
```

6.1.4.6 pk

```
List<ECPoint> at.iaik.mpc_acc.Accumulator.pk [private]
```

Generated by Doxygen

6.2 at.iaik.mpc_acc.AccumulatorDemo Class Reference

6.1.4.7 pk2

ECPoint at.iaik.mpc_acc.Accumulator.pk2 [private]

6.1.4.8 Q

final BigInteger at.iaik.mpc_acc.Accumulator.Q [private]

6.1.4.9 random

SecureRandom at.iaik.mpc_acc.Accumulator.random [private]

6.1.4.10 size

int at.iaik.mpc_acc.Accumulator.size [private]

6.1.4.11 t

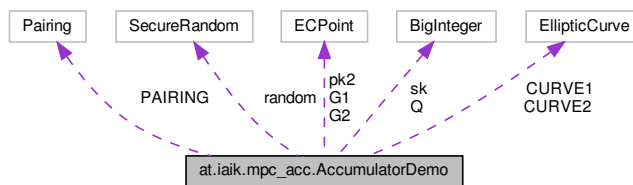
int at.iaik.mpc_acc.Accumulator.t [private]

The documentation for this class was generated from the following file:

- [Accumulator.java](#)

6.2 at.iaik.mpc_acc.AccumulatorDemo Class Reference

Collaboration diagram for at.iaik.mpc_acc.AccumulatorDemo:



Public Member Functions

- [AccumulatorDemo](#) (int *size*)
- void [test](#) (List< BigInteger > *X*)

Private Member Functions

- BigInteger [getRandomScalar](#) ()
- void [Gen](#) ()
- [EvalResult Eval](#) (List< BigInteger > *X*)
- ECPoint [WitCreate](#) (ECPoint *acc*, [Auxillery](#) *aux*, BigInteger *x*)
- Boolean [Verify](#) (ECPoint *acc*, ECPoint *wit*, BigInteger *x*)
- [EvalResult Add](#) (ECPoint *acc*, [Auxillery](#) *aux*, BigInteger *x*)
- [EvalResult Delete](#) (ECPoint *acc*, [Auxillery](#) *aux*, BigInteger *x*)
- ECPoint [WitUpdate](#) (ECPoint *wit*, [Auxillery](#) *aux*, BigInteger *x*)

Private Attributes

- final Pairing [PAIRING](#)
- final EllipticCurve [CURVE1](#)
- final EllipticCurve [CURVE2](#)
- final BigInteger [Q](#)
- final ECPoint [G1](#)
- final ECPoint [G2](#)
- int [size](#)
- ECPoint [pk2](#)
- BigInteger [sk](#)
- SecureRandom [random](#)

6.2.1 Detailed Description

A simple class computing the non-MPC accumulator using the secret key.

Author

Roman Walch

6.2.2 Constructor & Destructor Documentation**6.2.2.1 AccumulatorDemo()**

```
at.iaik.mpc_acc.AccumulatorDemo.AccumulatorDemo (  
    int size )
```

Constructor

Generated by Doxygen

Parameters

<i>size</i>	bitlength of the used pairing curves (400)
-------------	--

6.2.3 Member Function Documentation

6.2.3.1 Add()

```
EvalResult at.iaik.mpc_acc.AccumulatorDemo.Add (
    ECPPoint acc,
    Auxillary aux,
    BigInteger x ) [private]
```

Adds an element to the accumulator

Parameters

<i>acc</i>	the accumulator
<i>aux</i>	the AUX data
<i>x</i>	the element

Returns

the new accumulator and AUX data

6.2.3.2 Delete()

```
EvalResult at.iaik.mpc_acc.AccumulatorDemo.Delete (
    ECPPoint acc,
    Auxillary aux,
    BigInteger x ) [private]
```

Removes an element from the accumulator

Parameters

<i>acc</i>	the accumulator
<i>aux</i>	the AUX data
<i>x</i>	the element

Returns

the new accumulator and AUX data

6.2.3.3 Eval()

```
EvalResult at.iaik.mpc_acc.AccumulatorDemo.Eval (  
    List< BigInteger > X ) [private]
```

Accumulates a set of elements into an accumulator

Parameters

X	the set of elements
---	---------------------

Returns

the accumulator and the AUX data

6.2.3.4 Gen()

```
void at.iaik.mpc_acc.AccumulatorDemo.Gen ( ) [private]
```

Generates the keys of the accumulator

6.2.3.5 getRandomScalar()

```
BigInteger at.iaik.mpc_acc.AccumulatorDemo.getRandomScalar ( ) [private]
```

Sample a random integer

Returns

a random integer

6.2.3.6 test()

```
void at.iaik.mpc_acc.AccumulatorDemo.test (  
    List< BigInteger > X )
```

A simple member to test the accumulator

Parameters

X	the set to be accumulated
---	---------------------------

6.2.3.7 Verify()

```
Boolean at.iaik.mpc_acc.AccumulatorDemo.Verify (  
    ECPPoint acc,
```

Generated by Doxygen


```
ECPoint wit,
BigInteger x ) [private]
```

Verifies if an element is part of the accumulator

Parameters

<i>acc</i>	the accumulator
<i>wit</i>	the witness to the element
<i>x</i>	the element

Returns

true if the element is part of the accumulator, false otherwise

6.2.3.8 WitCreate()

```
ECPoint at.iaik.mpc_acc.AccumulatorDemo.WitCreate (
    ECPoint acc,
    Auxillery aux,
    BigInteger x ) [private]
```

Creates a [Witness](#) to an element in the accumulator

Parameters

<i>acc</i>	the accumulator
<i>aux</i>	the AUX data
<i>x</i>	the element in the accumulator

Returns

the witness to the element

6.2.3.9 WitUpdate()

```
ECPoint at.iaik.mpc_acc.AccumulatorDemo.WitUpdate (
    ECPoint wit,
    Auxillery aux,
    BigInteger x ) [private]
```

Updates a witness after element addition/removal

Parameters

<i>wit</i>	the previous witness of the element
<i>aux</i>	the AUX data
<i>x</i>	the element

Returns

the updated witness

6.2.4 Member Data Documentation

6.2.4.1 CURVE1

```
final EllipticCurve at.iaik.mpc_acc.AccumulatorDemo.CURVE1 [private]
```

6.2.4.2 CURVE2

```
final EllipticCurve at.iaik.mpc_acc.AccumulatorDemo.CURVE2 [private]
```

6.2.4.3 G1

```
final ECPoint at.iaik.mpc_acc.AccumulatorDemo.G1 [private]
```

6.2.4.4 G2

```
final ECPoint at.iaik.mpc_acc.AccumulatorDemo.G2 [private]
```

6.2.4.5 PAIRING

```
final Pairing at.iaik.mpc_acc.AccumulatorDemo.PAIRING [private]
```

6.2.4.6 pk2

```
ECPoint at.iaik.mpc_acc.AccumulatorDemo.pk2 [private]
```

6.2.4.7 Q

```
final BigInteger at.iaik.mpc_acc.AccumulatorDemo.Q [private]
```

Generated by Doxygen

6.2.4.8 random

```
SecureRandom at.iaik.mpc_acc.AccumulatorDemo.random [private]
```

6.2.4.9 size

```
int at.iaik.mpc_acc.AccumulatorDemo.size [private]
```

6.2.4.10 sk

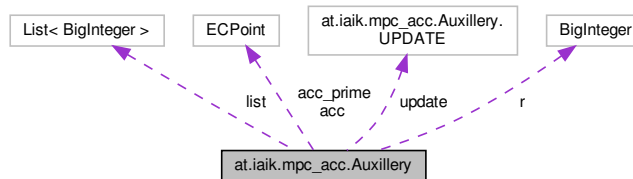
```
BigInteger at.iaik.mpc_acc.AccumulatorDemo.sk [private]
```

The documentation for this class was generated from the following file:

- [AccumulatorDemo.java](#)

6.3 at.iaik.mpc_acc.Auxillery Class Reference

Collaboration diagram for at.iaik.mpc_acc.Auxillery:



Classes

- enum **UPDATE**

Public Member Functions

- [Auxillery](#) (List< BigInteger > [list](#), UPDATE [update](#))
- [Auxillery](#) (List< BigInteger > [list](#), UPDATE [update](#), ECPoint [acc](#), ECPoint [acc_prime](#))
- [Auxillery](#) (List< BigInteger > [list](#), BigInteger [r](#))
- List< BigInteger > [getList](#) ()
- UPDATE [getUpdate](#) ()
- void [clearUpdate](#) ()
- BigInteger [getR](#) ()
- ECPoint [getAcc](#) ()
- ECPoint [getAccPrime](#) ()

Generated by Doxygen

Private Attributes

- List< BigInteger > [list](#)
- BigInteger [r](#)
- UPDATE [update](#)
- ECPoint [acc](#)
- ECPoint [acc_prime](#)

6.3.1 Detailed Description

A simple class containing the AUX data

Author

Roman Walch

6.3.2 Constructor & Destructor Documentation

6.3.2.1 Auxillery() [1/3]

```
at.iaik.mpc_acc.Auxillery.Auxillery (
    List< BigInteger > list,
    UPDATE update )
```

Initialize the class

Parameters

<i>list</i>	the list of elements
<i>update</i>	indicator if a add/delete operation was conducted

6.3.2.2 Auxillery() [2/3]

```
at.iaik.mpc_acc.Auxillery.Auxillery (
    List< BigInteger > list,
    UPDATE update,
    ECPoint acc,
    ECPoint acc_prime )
```

Initialize the class

Parameters

<i>list</i>	the list of elements
<i>update</i>	indicator if a add/delete operation was conducted
<i>acc</i>	the previous accumulator
<i>acc_prime</i>	the accumulator

Generated by Doxygen

6.3.2.3 Auxillery() [3/3]

```
at.iaik.mpc_acc.Auxillery.Auxillery (
    List< BigInteger > list,
    BigInteger r )
```

Initialize the class

Parameters

<i>list</i>	the list of elements
<i>r</i>	the random element

6.3.3 Member Function Documentation

6.3.3.1 clearUpdate()

```
void at.iaik.mpc_acc.Auxillery.clearUpdate ( )
```

Clears the update indicator

6.3.3.2 getAcc()

```
ECPoint at.iaik.mpc_acc.Auxillery.getAcc ( )
```

Getter for the previous accumulator

6.3.3.3 getAccPrime()

```
ECPoint at.iaik.mpc_acc.Auxillery.getAccPrime ( )
```

Getter for the accumulator

6.3.3.4 getList()

```
List<BigInteger> at.iaik.mpc_acc.Auxillery.getList ( )
```

Getter for the list of elements

6.3.3.5 getR()

```
BigInteger at.iaik.mpc_acc.Auxillery.getR ( )
```

Getter for the random element

Generated by Doxygen

6.3.3.6 getUpdate()

```
UPDATE at.iaik.mpc_acc.Auxillery.getUpdate ( )
```

Getter for the update indicator

6.3.4 Member Data Documentation

6.3.4.1 acc

```
ECPoint at.iaik.mpc_acc.Auxillery.acc [private]
```

6.3.4.2 acc_prime

```
ECPoint at.iaik.mpc_acc.Auxillery.acc_prime [private]
```

6.3.4.3 list

```
List<BigInteger> at.iaik.mpc_acc.Auxillery.list [private]
```

6.3.4.4 r

```
BigInteger at.iaik.mpc_acc.Auxillery.r [private]
```

6.3.4.5 update

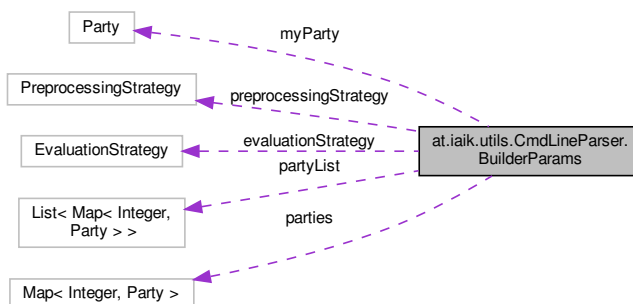
```
UPDATE at.iaik.mpc_acc.Auxillery.update [private]
```

The documentation for this class was generated from the following file:

- [Auxillery.java](#)

6.4 at.iaik.utils.CmdLineParser.BuilderParams Class Reference

Collaboration diagram for at.iaik.utils.CmdLineParser.BuilderParams:



Public Member Functions

- `BuilderParams` (boolean `logging`, boolean `multiThreaded`)
- void `setId` (int `id`)
- void `setEl` (int `el`)
- void `setParties` (List< Map< Integer, Party >> `partyList`, Party `party`)
- void `setMaxBitLength` (int `maxBitLength`)
- void `setPreprocessingStrategy` (PreprocessingStrategy `strategy`)
- void `setEvaluationStrategy` (EvaluationStrategy `strategy`)

Public Attributes

- boolean `logging`
- int `id`
- Party `myParty`
- Map< Integer, Party > `parties`
- List< Map< Integer, Party >> `partyList`
- int `maxBitLength`
- PreprocessingStrategy `preprocessingStrategy`
- EvaluationStrategy `evaluationStrategy`
- boolean `multiThreaded`
- int `el`

6.4.1 Detailed Description

A class providing storage for all the parameters the applications need to be properly initialized. This includes parameters used in the framework as well as parameters which are use case specific.

6.4.2 Constructor & Destructor Documentation

6.4.2.1 BuilderParams()

```
at.iaik.utils.CmdLineParser.BuilderParams.BuilderParams (
    boolean logging,
    boolean multiThreaded )
```

6.4.3 Member Function Documentation

6.4.3.1 setEl()

```
void at.iaik.utils.CmdLineParser.BuilderParams.setEl (
    int el )
```

6.4.3.2 setEvaluationStrategy()

```
void at.iaik.utils.CmdLineParser.BuilderParams.setEvaluationStrategy (
    EvaluationStrategy strategy )
```

6.4.3.3 setId()

```
void at.iaik.utils.CmdLineParser.BuilderParams.setId (
    int id )
```

6.4.3.4 setMaxBitLength()

```
void at.iaik.utils.CmdLineParser.BuilderParams.setMaxBitLength (
    int maxBitLength )
```

6.4.3.5 setParties()

```
void at.iaik.utils.CmdLineParser.BuilderParams.setParties (
    List< Map< Integer, Party >> partyList,
    Party party )
```


6.4.3.6 setPreprocessingStrategy()

```
void at.iaik.utils.CmdLineParser.BuilderParams.setPreprocessingStrategy (
    PreprocessingStrategy strategy )
```

6.4.4 Member Data Documentation

6.4.4.1 el

```
int at.iaik.utils.CmdLineParser.BuilderParams.el
```

6.4.4.2 evaluationStrategy

```
EvaluationStrategy at.iaik.utils.CmdLineParser.BuilderParams.evaluationStrategy
```

6.4.4.3 id

```
int at.iaik.utils.CmdLineParser.BuilderParams.id
```

6.4.4.4 logging

```
boolean at.iaik.utils.CmdLineParser.BuilderParams.logging
```

6.4.4.5 maxBitLength

```
int at.iaik.utils.CmdLineParser.BuilderParams.maxBitLength
```

6.4.4.6 multiThreaded

```
boolean at.iaik.utils.CmdLineParser.BuilderParams.multiThreaded
```

6.4.4.7 myParty

```
Party at.iaik.utils.CmdLineParser.BuilderParams.myParty
```

Generated by Doxygen

6.4.4.8 parties

```
Map<Integer, Party> at.iaik.utils.CmdLineParser.BuilderParams.parties
```

6.4.4.9 partyList

```
List<Map<Integer, Party> > at.iaik.utils.CmdLineParser.BuilderParams.partyList
```

6.4.4.10 preprocessingStrategy

```
PreprocessingStrategy at.iaik.utils.CmdLineParser.BuilderParams.preprocessingStrategy
```

The documentation for this class was generated from the following file:

- [CmdLineParser.java](#)

6.5 at.iaik.utils.CmdLineParser Class Reference

Classes

- class [BuilderParams](#)

Static Public Member Functions

- static Party [checkParty](#) (String partyOption) throws ParseException
- static [BuilderParams GetCmdLineParams](#) (String[] args) throws ParseException

Static Public Attributes

- static final String [IDMSG](#) = "The id of this player. Must be a unique positive integer."
- static final String [SETMSG](#) = "The number of elements in the generator."
- static final String [PARTYMSG](#) = "Connection data for a party. Use -p multiple times to specify many players. You must always at least include yourself. Must be on the form [id]:[hostname]:[port]. id is a unique positive integer for the player, host and port is where to find the player"
- static final String [PRESTRATMSG](#) = "Used to set the preprocessing Strategy of SPDZ"
- static final String [LOGGINGMSG](#) = "Informs FRESCO that performance logging should be triggered"
- static final String [IDERRMSG](#) = "ID must be positive"
- static final String [PARTYERRMSG](#) = "Party ids must be unique"
- static final String [SETERRMSG](#) = "number of elements must be > 1"
- static int [newID](#) = 0

Static Private Member Functions

- static List< Map< Integer, Party > > [createPartyMap](#) (Map< Integer, Party > parties, int myID)

Generated by Doxygen

6.5.1 Detailed Description

Utility class to gather all the builder parameters necessary for the applications from the command line.

Author

Fabian Schmid

6.5.2 Member Function Documentation

6.5.2.1 checkParty()

```
static Party at.iaik.utils.CmdLineParser.checkParty (
    String partyOption ) throws ParseException [static]
```

Checks on a basic level if the party input after -p is in the correct form

Parameters

<i>partyOption</i>	The option provided after this -p argument
--------------------	--

Returns

Returns the party parsed from the partyOption

Exceptions

<i>ParseException</i>	If the partyOption is not compliant with the expected format
-----------------------	--

6.5.2.2 createPartyMap()

```
static List<Map<Integer, Party> > at.iaik.utils.CmdLineParser.createPartyMap (
    Map< Integer, Party > parties,
    int myID ) [static], [private]
```

In case the application is executed using multi threading, this function separates the parties into different party maps. in these different maps, the ids are newly set, since in the framework the ids have to contain 1 and have to ascend from one on. If this is to be changed, one has to replace the socket network of the framework with an independent implementation.

Parameters

<i>parties</i>	the current party map which is to be separated
<i>myID</i>	the id this user currently possesses

Returns

a list of new party maps, one for each subgroup of clients

NOTE: This function has to be exchanged/modified if one wants to change the logic of separation (e.g. separation by date) Now separation is by id: (1,2,3), (1,4,5) ... 1 is infineon and has to be present in every map

6.5.2.3 GetCmdLineParams()

```
static BuilderParams at.iaik.utils.CmdLineParser.GetCmdLineParams (
    String [] args ) throws ParseException [static]
```

Main functionality to read the input arguments and parse the Builder Parameters. Every option is required but the multithreaded and logging flag. the correct format of each option can be read below or int the examples given in the makefile

Parameters

<i>args</i>	the command line arguments provided when starting up the program
-------------	--

Returns

Returns a [BuilderParams](#) object, providing everything the builders need.

Exceptions

<i>ParseException</i>	throws this exception if some value is not as expected
-----------------------	--

6.5.3 Member Data Documentation**6.5.3.1 IDERRMSG**

```
final String at.iaik.utils.CmdLineParser.IDERRMSG = "ID must be positive" [static]
```

6.5.3.2 IDMSG

```
final String at.iaik.utils.CmdLineParser.IDMSG = "The id of this player. Must be a unique positive integer." [static]
```

6.5.3.3 LOGGINGMSG

```
final String at.iaik.utils.CmdLineParser.LOGGINGMSG = "Informs FRESCO that performance logging should be triggered" [static]
```

6.5.3.4 newID

```
int at.iaik.utils.CmdLineParser.newID = 0 [static]
```

6.5.3.5 PARTYERRMSG

```
final String at.iaik.utils.CmdLineParser.PARTYERRMSG = "Party ids must be unique" [static]
```

6.5.3.6 PARTYMSG

```
final String at.iaik.utils.CmdLineParser.PARTYMSG = "Connection data for a party. Use -p multiple times to specify many players. You must always at least include yourself. Must be on the form [id]:[hostname]:[port]. id is a unique positive integer for the player, host and port is where to find the player" [static]
```

6.5.3.7 PRESTRATMSG

```
final String at.iaik.utils.CmdLineParser.PRESTRATMSG = "Used to set the preprocessing Strategy of SPDZ" [static]
```

6.5.3.8 SETERRMSG

```
final String at.iaik.utils.CmdLineParser.SETERRMSG = "number of elements must be > 1" [static]
```

6.5.3.9 SETMSG

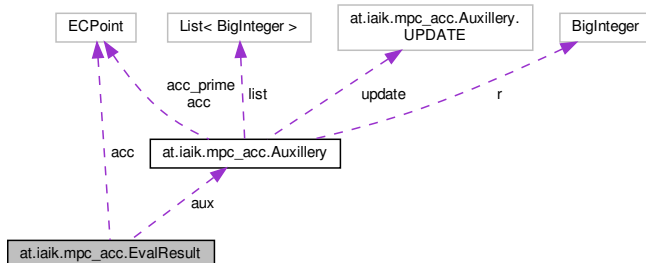
```
final String at.iaik.utils.CmdLineParser.SETMSG = "The number of elements in the generator." [static]
```

The documentation for this class was generated from the following file:

- [CmdLineParser.java](#)

6.6 at.iaik.mpc_acc.EvalResult Class Reference

Collaboration diagram for at.iaik.mpc_acc.EvalResult:



Public Member Functions

- [EvalResult](#) (ECPoint [acc](#), List< BigInteger > [list](#))
- [EvalResult](#) (ECPoint [acc](#), List< BigInteger > [list](#), Auxillery.UPDATE [update](#))
- [EvalResult](#) (ECPoint [acc](#), List< BigInteger > [list](#), Auxillery.UPDATE [update](#), ECPoint [acc_old](#))
- [EvalResult](#) (ECPoint [acc](#), List< BigInteger > [list](#), BigInteger [r](#))
- ECPoint [getAcc](#) ()
- Auxillery [getAuxillery](#) ()

Private Attributes

- ECPoint [acc](#)
- Auxillery [aux](#)

6.6.1 Detailed Description

A simple class containing the evaluation result

Author

Roman Walch

6.6.2 Constructor & Destructor Documentation

6.6.2.1 EvalResult() [1/4]

```

at.iaik.mpc_acc.EvalResult.EvalResult (
    ECPoint acc,
    List< BigInteger > list )
  
```

Initialize the class

Parameters

<i>acc</i>	the accumulator
<i>list</i>	the list of elements in the accumulator

6.6.2.2 EvalResult() [2/4]

```
at.iaik.mpc_acc.EvalResult.EvalResult (
    ECPoint acc,
    List< BigInteger > list,
    Auxillery.UPDATE update )
```

Initialize the class

Parameters

<i>acc</i>	the accumulator
<i>list</i>	the list of elements in the accumulator
<i>update</i>	specifies if a add/delete operation was conducted

6.6.2.3 EvalResult() [3/4]

```
at.iaik.mpc_acc.EvalResult.EvalResult (
    ECPoint acc,
    List< BigInteger > list,
    Auxillery.UPDATE update,
    ECPoint acc_old )
```

Initialize the class

Parameters

<i>acc</i>	the accumulator
<i>list</i>	the list of elements in the accumulator
<i>update</i>	specifies if a add/delete operation was conducted
<i>acc_old</i>	the previous accumulator

6.6.2.4 EvalResult() [4/4]

```
at.iaik.mpc_acc.EvalResult.EvalResult (
    ECPoint acc,
    List< BigInteger > list,
    BigInteger r )
```

Initialize the class

Parameters

<i>acc</i>	the accumulator
<i>list</i>	the list of elements in the accumulator
<i>r</i>	the random element

6.6.3 Member Function Documentation

6.6.3.1 getAcc()

`ECPoint at.iaik.mpc_acc.EvalResult.getAcc ()`

Getter for the accumulator

6.6.3.2 getAuxillery()

`Auxillery at.iaik.mpc_acc.EvalResult.getAuxillery ()`

Getter for the AUX data

6.6.4 Member Data Documentation

6.6.4.1 acc

`ECPoint at.iaik.mpc_acc.EvalResult.acc [private]`

6.6.4.2 aux

`Auxillery at.iaik.mpc_acc.EvalResult.aux [private]`

The documentation for this class was generated from the following file:

- [EvalResult.java](#)

6.7 at.iaik.mpc_acc.Main Class Reference

Static Public Member Functions

- static void [main](#) (String[] args) throws ParseException

Static Private Member Functions

- static List< BigInteger > [genList](#) (BigInteger mod, int elements)

Static Private Attributes

- static final int [SIZE](#) = 400

6.7.1 Detailed Description

A simple demo computing the MPC accumulator.

Author

Roman Walch

6.7.2 Member Function Documentation**6.7.2.1 genList()**

```
static List<BigInteger> at.iaik.mpc_acc.Main.genList (
    BigInteger mod,
    int elements ) [static], [private]
```

A simple member to generate a set to be accumulated

Parameters

<i>mod</i>	the used modulus
<i>elements</i>	the number of elements

Returns

the list of elements

6.7.2.2 main()

```
static void at.iaik.mpc_acc.Main.main (
    String [] args ) throws ParseException [static]
```

The main class to test the MPC accumulator implementation

Exceptions

<i>ParseException</i>	
-----------------------	--

Generated by Doxygen

6.7.3 Member Data Documentation

6.7.3.1 SIZE

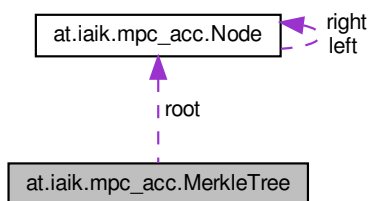
```
final int at.iaik.mpc_acc.Main.SIZE = 400 [static], [private]
```

The documentation for this class was generated from the following file:

- [Main.java](#)

6.8 at.iaik.mpc_acc.MerkleTree Class Reference

Collaboration diagram for at.iaik.mpc_acc.MerkleTree:



Classes

- enum [Position](#)
- class [ProofNode](#)

Public Member Functions

- [MerkleTree](#) (List< byte[] > hashes)
- [MerkleTree](#) (byte[] root_hash)
- List< [ProofNode](#) > [proof](#) (byte[] digest)
- Boolean [verify](#) (byte[] element, List< [ProofNode](#) > proof)
- byte [] [getRootHash](#) ()

Static Public Member Functions

- static void [test](#) (List< BigInteger > X)

Generated by Doxygen

Private Member Functions

- Boolean `find` (`Node` node, `Stack`< `Pair`< `Position`, `Node` >> nodes, `byte`[] digest)

Static Private Member Functions

- static int `round_up_to_power_of_2` (int value)

Private Attributes

- `Node` `root`
the root node of the merkle tree

6.8.1 Detailed Description

A simple class for Merkle Tree accumulators

Author

Roman Walch

6.8.2 Constructor & Destructor Documentation

6.8.2.1 `MerkleTree()` [1/2]

```
at.iaik.mpc_acc.MerkleTree.MerkleTree (
    List< byte[]> hashes )
```

Initialize Merkle tree from a set of digests.

Given the vector of digest, builds a Merkle tree where the digests are placed in the the leaf nodes.

Parameters

<code>hashes</code>	set of digests, which will be hashed into the leaf nodes
---------------------	--

6.8.2.2 `MerkleTree()` [2/2]

```
at.iaik.mpc_acc.MerkleTree.MerkleTree (
    byte [] root_hash )
```

Initialize Merkle tree from a root hash.

In this configuration, the Merkle tree can only be used for verification.

Parameters

<code>root_hash</code>	the root hash
------------------------	---------------

6.8.3 Member Function Documentation

6.8.3.1 find()

```
Boolean at.iaik.mpc_acc.MerkleTree.find (
    Node node,
    Stack< Pair< Position, Node >> nodes,
    byte [] digest ) [private]
```

6.8.3.2 getRootHash()

```
byte [] at.iaik.mpc_acc.MerkleTree.getRootHash ( )
```

Return root hash of the Merkle tree

Returns

root hash

6.8.3.3 proof()

```
List<ProofNode> at.iaik.mpc_acc.MerkleTree.proof (
    byte [] digest )
```

Create a member ship proof for the given digest.

A proof consists of a sequence of proof_node instances, where each proof_node declares if the proven value is the left or right input to the hash function and contains the digest of the sibling.

Parameters

<code>digest</code>	digest to proof
---------------------	-----------------

Returns

sequence of proof nodes or an empty sequence of the value is not contained in the tree

6.8.3.4 round_up_to_power_of_2()

```
static int at.iaik.mpc_acc.MerkleTree.round_up_to_power_of_2 (
    int value ) [static], [private]
```

6.8.3.5 test()

```
static void at.iaik.mpc_acc.MerkleTree.test (
    List< BigInteger > X ) [static]
```

A simple member to test the merkle tree

Parameters

X	the set to be accumulated
---	---------------------------

6.8.3.6 verify()

```
Boolean at.iaik.mpc_acc.MerkleTree.verify (
    byte [] element,
    List< ProofNode > proof )
```

Verify the membership of a given value and its proof against the root hash.

Parameters

<i>element</i>	value to be tested
<i>proof</i>	proof for the given value

Returns

true if the value is contained in the tree, i.e. the proof matches the root hash

6.8.4 Member Data Documentation

6.8.4.1 root

```
Node at.iaik.mpc_acc.MerkleTree.root [private]
```

the root node of the merkle tree

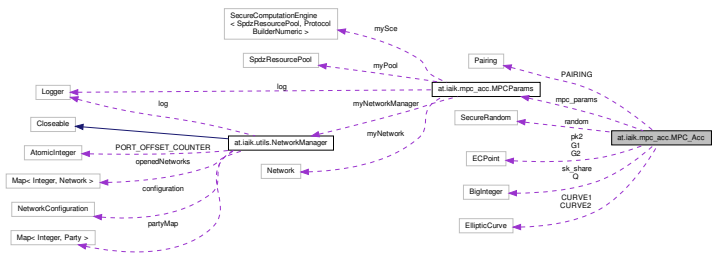
The documentation for this class was generated from the following file:

- [MerkleTree.java](#)

Generated by Doxygen

6.9 at.iaik.mpc_acc.MPC_Acc Class Reference

Collaboration diagram for at.iaik.mpc_acc.MPC_Acc:



Public Member Functions

- BigInteger `getRandomScalar` ()
- `MPC_Acc` (int `size`, CmdLineParser.BuilderParams `params`) throws `ParseException`
- void `gen` ()
- `EvalResult` `eval` (List< BigInteger > `X`)
- `Witness` `witCreate` (ECPoint `acc`, `Auxillary` `aux`, BigInteger `x`)
- Boolean `verify` (ECPoint `acc`, `Witness` `wit`, BigInteger `x`)
- `EvalResult` `add` (ECPoint `acc`, `Auxillary` `aux`, BigInteger `x`)
- `EvalResult` `delete` (ECPoint `acc`, `Auxillary` `aux`, BigInteger `x`)
- `Witness` `witUpdate` (`Witness` `wit`, `Auxillary` `aux`, BigInteger `x`)
- void `close` ()
- void `printAndResetComm` (String `info`)
- void `prepareBatches` (int `mul`, int `random`)
- BigInteger `getQ` ()

Private Attributes

- final Pairing `PAIRING`
- final EllipticCurve `CURVE1`
- final EllipticCurve `CURVE2`
- final BigInteger `Q`
- final ECPoint `G1`
- final ECPoint `G2`
- int `size`
- ECPoint `pk2`
- `MPCParams` `mpc_params`
- BigInteger `sk_share`
- `SecureRandom` `random`

6.9.1 Detailed Description

A simple demo for the MPC accumulator computations

Author

Roman Walch

Generated by Doxygen

6.9.2 Constructor & Destructor Documentation

6.9.2.1 MPC_Acc()

```
at.iaik.mpc_acc.MPC_Acc.MPC_Acc (
    int size,
    CommandLineParser.BuilderParams params ) throws ParseException
```

Constructor

Parameters

<i>size</i>	bitlength of the used pairing curves (400)
<i>params</i>	command line params to specify the computation parameters

6.9.3 Member Function Documentation

6.9.3.1 add()

```
EvalResult at.iaik.mpc_acc.MPC_Acc.add (
    ECPPoint acc,
    Auxillary aux,
    BigInteger x )
```

Adds an element to the accumulator

Parameters

<i>acc</i>	the accumulator
<i>aux</i>	the AUX data
<i>x</i>	the element

Returns

the new accumulator and AUX data

6.9.3.2 close()

```
void at.iaik.mpc_acc.MPC_Acc.close ( )
```

Closes the network and secure computation engine

6.9.3.3 delete()

```
EvalResult at.iaik.mpc_acc.MPC_Acc.delete (
    ECPoint acc,
    Auxillary aux,
    BigInteger x )
```

Removes an element from the accumulator

Parameters

<i>acc</i>	the accumulator
<i>aux</i>	the AUX data
<i>x</i>	the element

Returns

the new accumulator and AUX data

6.9.3.4 eval()

```
EvalResult at.iaik.mpc_acc.MPC_Acc.eval (
    List< BigInteger > X )
```

Accumulates a set of elements into an accumulator

Parameters

<i>X</i>	the set of elements
----------	---------------------

Returns

the accumulator and the AUX data

6.9.3.5 gen()

```
void at.iaik.mpc_acc.MPC_Acc.gen ( )
```

Generates the keys of the accumulator

6.9.3.6 getQ()

```
BigInteger at.iaik.mpc_acc.MPC_Acc.getQ ( )
```

Getter for the modulus

6.9.3.7 getRandomScalar()

```
BigInteger at.iaik.mpc_acc.MPC_Acc.getRandomScalar ( )
```

Sample a random integer

Returns

a random integer

6.9.3.8 prepareBatches()

```
void at.iaik.mpc_acc.MPC_Acc.prepareBatches (
    int mul,
    int random )
```

Precomputes shared random elements and beaver triples during the offline phase

Parameters

<i>mul</i>	the number of beaver triples to be produced
<i>random</i>	the number of shared random elements to be produced

6.9.3.9 printAndResetComm()

```
void at.iaik.mpc_acc.MPC_Acc.printAndResetComm (
    String info )
```

Prints the currently communicated bytes and reset the counter

Parameters

<i>info</i>	Output prefix
-------------	---------------

6.9.3.10 verify()

```
Boolean at.iaik.mpc_acc.MPC_Acc.verify (
    ECPoint acc,
    Witness wit,
    BigInteger x )
```

Verifies if an element is part of the accumulator

Parameters

<i>acc</i>	the accumulator
<i>wit</i>	the witness to the element
<i>x</i>	the element

Returns

true if the element is part of the accumulator, false otherwise

6.9.3.11 witCreate()

```
Witness at.iaik.mpc_acc.MPC_Acc.witCreate (
    ECPPoint acc,
    Auxillery aux,
    BigInteger x )
```

Creates a **Witness** to an element in the accumulator

Parameters

<i>acc</i>	the accumulator
<i>aux</i>	the AUX data
<i>x</i>	the element in the accumulator

Returns

the witness to the element

6.9.3.12 witUpdate()

```
Witness at.iaik.mpc_acc.MPC_Acc.witUpdate (
    Witness wit,
    Auxillery aux,
    BigInteger x )
```

Updates a witness after element addition/removal

Parameters

<i>wit</i>	the previous witness of the element
<i>aux</i>	the AUX data
<i>x</i>	the element

Returns

the updated witness

6.9.4 Member Data Documentation

6.9.4.1 CURVE1

```
final EllipticCurve at.iaik.mpc_acc.MPC_Acc.CURVE1 [private]
```

6.9.4.2 CURVE2

```
final EllipticCurve at.iaik.mpc_acc.MPC_Acc.CURVE2 [private]
```

6.9.4.3 G1

```
final ECPoint at.iaik.mpc_acc.MPC_Acc.G1 [private]
```

6.9.4.4 G2

```
final ECPoint at.iaik.mpc_acc.MPC_Acc.G2 [private]
```

6.9.4.5 mpc_params

```
MPCParams at.iaik.mpc_acc.MPC_Acc.mpc_params [private]
```

6.9.4.6 PAIRING

```
final Pairing at.iaik.mpc_acc.MPC_Acc.PAIRING [private]
```

6.9.4.7 pk2

```
ECPoint at.iaik.mpc_acc.MPC_Acc.pk2 [private]
```

6.9.4.8 Q

```
final BigInteger at.iaik.mpc_acc.MPC_Acc.Q [private]
```

6.9.4.9 random

```
SecureRandom at.iaik.mpc_acc.MPC_Acc.random [private]
```

Generated by Doxygen

6.9.4.10 size

```
int at.iaik.mpc_acc.MPC_Acc.size [private]
```

6.9.4.11 sk_share

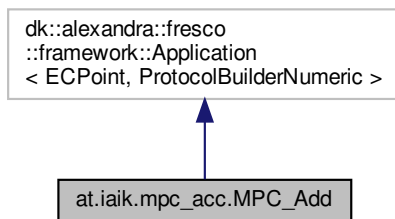
```
BigInteger at.iaik.mpc_acc.MPC_Acc.sk_share [private]
```

The documentation for this class was generated from the following file:

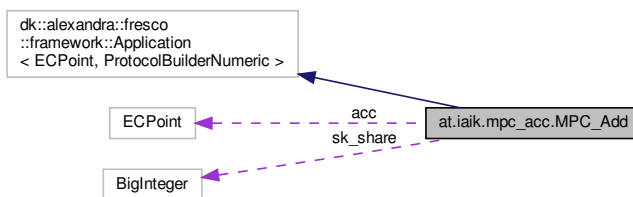
- [MPC_Acc.java](#)

6.10 at.iaik.mpc_acc.MPC_Add Class Reference

Inheritance diagram for at.iaik.mpc_acc.MPC_Add:



Collaboration diagram for at.iaik.mpc_acc.MPC_Add:



Public Member Functions

- [MPC_Add](#) (BigInteger [sk_share](#), ECPoint [acc](#))
- DRes< ECPoint > [buildComputation](#) (ProtocolBuilderNumeric producer)

Generated by Doxygen

Private Attributes

- BigInteger *sk_share*
- ECPoint *acc*

6.10.1 Detailed Description

Implements the functionality to add an element to the accumulator

Author

Roman Walch

6.10.2 Constructor & Destructor Documentation**6.10.2.1 MPC_Add()**

```
at.iaik.mpc_acc.MPC_Add.MPC_Add (  
    BigInteger sk_share,  
    ECPoint acc )
```

Construct a add computation object for element addition

Parameters

<i>sk_share</i>	the shared secret key
<i>x</i>	the element to be added
<i>acc</i>	the accumulator

6.10.3 Member Function Documentation**6.10.3.1 buildComputation()**

```
DRes<ECPoint> at.iaik.mpc_acc.MPC_Add.buildComputation (  
    ProtocolBuilderNumeric producer )
```

Performs the MPC computation to add an element to the accumulator

Returns

the updated accumulator

6.10.4 Member Data Documentation

Generated by Doxygen

6.11 at.iaik.mpc_acc.MPC_Del Class Reference

6.10.4.1 acc

ECPoint at.iaik.mpc_acc.MPC_Add.acc [private]

6.10.4.2 sk_share

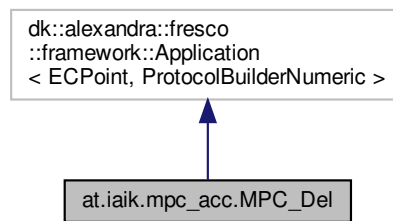
BigInteger at.iaik.mpc_acc.MPC_Add.sk_share [private]

The documentation for this class was generated from the following file:

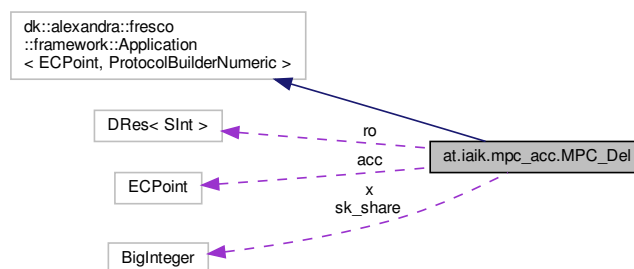
- [MPC_Add.java](#)

6.11 at.iaik.mpc_acc.MPC_Del Class Reference

Inheritance diagram for at.iaik.mpc_acc.MPC_Del:



Collaboration diagram for at.iaik.mpc_acc.MPC_Del:



Public Member Functions

- `MPC_Del` (BigInteger `sk_share`, BigInteger `x`, ECPoint `acc`)
- `DRes< ECPoint > buildComputation` (ProtocolBuilderNumeric producer)

Private Attributes

- BigInteger `sk_share`
- BigInteger `x`
- ECPoint `acc`
- `DRes< Sint > ro`

6.11.1 Detailed Description

Implements the functionality to delete an element from the accumulator

Author

Roman Walch

6.11.2 Constructor & Destructor Documentation**6.11.2.1 MPC_Del()**

```
at.iaik.mpc_acc.MPC_Del.MPC_Del (
    BigInteger sk_share,
    BigInteger x,
    ECPoint acc )
```

Construct a delete computation object for element removal

Parameters

<i>sk_share</i>	the shared secret key
<i>x</i>	the element to be removed
<i>acc</i>	the accumulator

6.11.3 Member Function Documentation**6.11.3.1 buildComputation()**

```
DRes<ECPoint> at.iaik.mpc_acc.MPC_Del.buildComputation (
    ProtocolBuilderNumeric producer )
```

Performs the MPC computation to remove an element from the accumulator

Generated by Doxygen

Returns

the updated accumulator

6.11.4 Member Data Documentation

6.11.4.1 acc

ECPoint at.iaik.mpc_acc.MPC_Del.acc [private]

6.11.4.2 ro

DRes<SInt> at.iaik.mpc_acc.MPC_Del.ro [private]

6.11.4.3 sk_share

BigInteger at.iaik.mpc_acc.MPC_Del.sk_share [private]

6.11.4.4 x

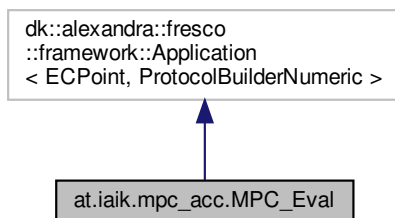
BigInteger at.iaik.mpc_acc.MPC_Del.x [private]

The documentation for this class was generated from the following file:

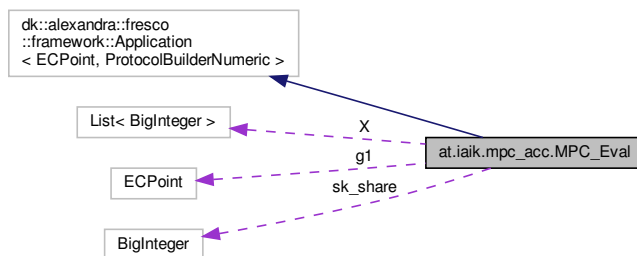
- [MPC_Del.java](#)

6.12 at.iaik.mpc_acc.MPC_Eval Class Reference

Inheritance diagram for at.iaik.mpc_acc.MPC_Eval:



Collaboration diagram for at.iaik.mpc_acc.MPC_Eval:



Public Member Functions

- `MPC_Eval` (`BigInteger sk_share`, `ECPoint g1`, `List< BigInteger > X`)
- `DRes< ECPoint > buildComputation` (`ProtocolBuilderNumeric` producer)

Private Attributes

- `BigInteger sk_share`
- `ECPoint g1`
- `List< BigInteger > X`

6.12.1 Detailed Description

Implements the functionality to create the accumulator from a set of values.

Author

Roman Walch

6.12.2 Constructor & Destructor Documentation

6.12.2.1 MPC_Eval()

```

at.iaik.mpc_acc.MPC_Eval.MPC_Eval (
    BigInteger sk_share,
    ECPoint g1,
    List< BigInteger > X )
  
```

Construct a eval computation object for creating the accumulator

Parameters

<i>sk_share</i>	the shared secret key
<i>g1</i>	the generator of the first pairing group
<i>X</i>	the list of elements to be accumulated

6.12.3 Member Function Documentation

6.12.3.1 buildComputation()

```
DRes<ECPoint> at.iaik.mpc_acc.MPC_Eval.buildComputation (
    ProtocolBuilderNumeric producer )
```

Performs the MPC computation to create the accumulator from the set of elements

Returns

the accumulator

6.12.4 Member Data Documentation

6.12.4.1 g1

```
ECPoint at.iaik.mpc_acc.MPC_Eval.g1 [private]
```

6.12.4.2 sk_share

```
BigInteger at.iaik.mpc_acc.MPC_Eval.sk_share [private]
```

6.12.4.3 X

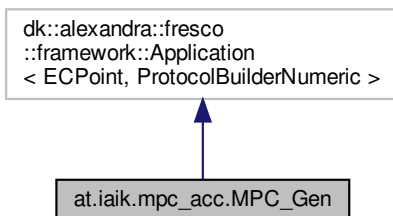
```
List<BigInteger> at.iaik.mpc_acc.MPC_Eval.X [private]
```

The documentation for this class was generated from the following file:

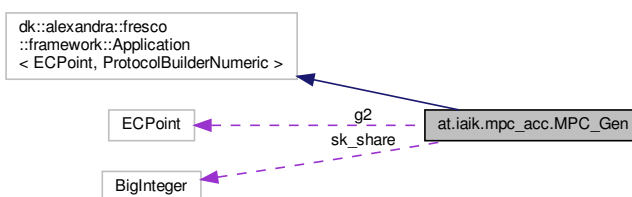
- [MPC_Eval.java](#)

6.13 at.iaik.mpc_acc.MPC_Gen Class Reference

Inheritance diagram for at.iaik.mpc_acc.MPC_Gen:



Collaboration diagram for at.iaik.mpc_acc.MPC_Gen:



Public Member Functions

- MPC_Gen (BigInteger sk_share, ECPoint g2)
- DRes< ECPoint > buildComputation (ProtocolBuilderNumeric producer)

Private Attributes

- BigInteger sk_share
- ECPoint g2

6.13.1 Detailed Description

Implements the functionality to generate the public key from the secret key shares

Author

Roman Walch

Generated by Doxygen

6.13.2 Constructor & Destructor Documentation

6.13.2.1 MPC_Gen()

```
at.iaik.mpc_acc.MPC_Gen.MPC_Gen (
    BigInteger sk_share,
    ECPoint g2 )
```

Construct a public key generation computation object

Parameters

<i>sk_share</i>	the shared secret key
<i>g2</i>	the generator of the second pairing group

6.13.3 Member Function Documentation

6.13.3.1 buildComputation()

```
DRes<ECPoint> at.iaik.mpc_acc.MPC_Gen.buildComputation (
    ProtocolBuilderNumeric producer )
```

Perform the MPC computation to create the public key from the shared secret key

Returns

the public key

6.13.4 Member Data Documentation

6.13.4.1 g2

```
ECPoint at.iaik.mpc_acc.MPC_Gen.g2 [private]
```

6.13.4.2 sk_share

```
BigInteger at.iaik.mpc_acc.MPC_Gen.sk_share [private]
```

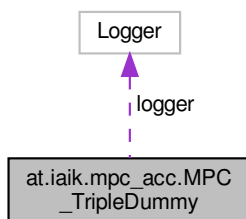
The documentation for this class was generated from the following file:

- [MPC_Gen.java](#)

Generated by Doxygen

6.14 at.iaik.mpc_acc.MPC_TripleDummy Class Reference

Collaboration diagram for at.iaik.mpc_acc.MPC_TripleDummy:



Static Public Member Functions

- static void [produceTriples](#) (SpdzMascotDataSupplier supplier, int elements)
- static void [produceRandomFieldElements](#) (SpdzMascotDataSupplier supplier, int elements)

Static Private Attributes

- static final int [LIMIT](#) = 1024
- static Logger [logger](#) = LoggerFactory.getLogger(MPC_TripleDummy.class)

6.14.1 Detailed Description

Dummy to create the batches of triples and random shares in the "offline" phase

Author

Roman Walch

6.14.2 Member Function Documentation

6.14.2.1 produceRandomFieldElements()

```

static void at.iaik.mpc_acc.MPC_TripleDummy.produceRandomFieldElements (
    SpdzMascotDataSupplier supplier,
    int elements ) [static]
  
```

Precomputes shared random elements in the offline phase

Generated by Doxygen

Parameters

<i>supplier</i>	the data supplier
<i>elements</i>	the number of shared random elements to be produced

6.14.2.2 produceTriples()

```
static void at.iaik.mpc_acc.MPC_TripleDummy.produceTriples (  
    SpdzMascotDataSupplier supplier,  
    int elements ) [static]
```

Precomputes shared triples in the offline phase

Parameters

<i>supplier</i>	the data supplier
<i>elements</i>	the number of triples to be produced

6.14.3 Member Data Documentation

6.14.3.1 LIMIT

```
final int at.iaik.mpc_acc.MPC_TripleDummy.LIMIT = 1024 [static], [private]
```

6.14.3.2 logger

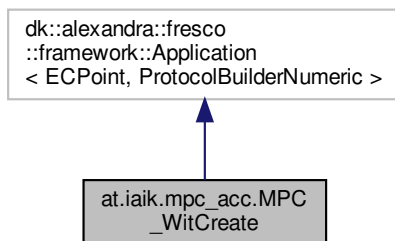
```
Logger at.iaik.mpc_acc.MPC_TripleDummy.logger = LoggerFactory.getLogger(MPC_TripleDummy.class)  
[static], [private]
```

The documentation for this class was generated from the following file:

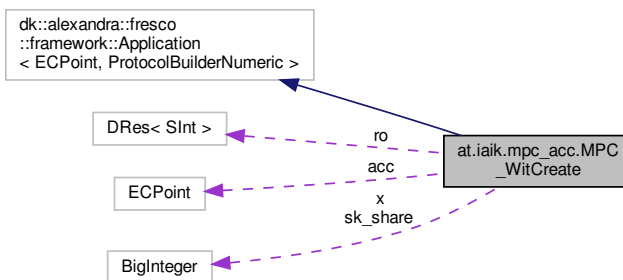
- [MPC_TripleDummy.java](#)

6.15 at.iaik.mpc_acc.MPC_WitCreate Class Reference

Inheritance diagram for at.iaik.mpc_acc.MPC_WitCreate:



Collaboration diagram for at.iaik.mpc_acc.MPC_WitCreate:



Public Member Functions

- MPC_WitCreate (BigInteger sk_share, BigInteger x, ECPoint acc)
- DRes< ECPoint > buildComputation (ProtocolBuilderNumeric producer)

Private Attributes

- BigInteger sk_share
- BigInteger x
- ECPoint acc
- DRes< SInt > ro

6.15.1 Detailed Description

Creates the witness to a member of the accumulator

Author

Roman Walch

6.15.2 Constructor & Destructor Documentation

6.15.2.1 MPC_WitCreate()

```
at.iaik.mpc_acc.MPC_WitCreate.MPC_WitCreate (
    BigInteger sk_share,
    BigInteger x,
    ECPoint acc )
```

Construct a witness computation object

Parameters

<i>sk_share</i>	the shared secret key
<i>x</i>	the element
<i>wit</i>	the accumulator

6.15.3 Member Function Documentation

6.15.3.1 buildComputation()

```
DRes<ECPoint> at.iaik.mpc_acc.MPC_WitCreate.buildComputation (
    ProtocolBuilderNumeric producer )
```

Performs the MPC computation to create a witness of a member of the accumulator

Returns

the witness of the element

6.15.4 Member Data Documentation

6.15.4.1 acc

```
ECPoint at.iaik.mpc_acc.MPC_WitCreate.acc [private]
```


6.15.4.2 ro

DRes<SInt> at.iaik.mpc_acc.MPC_WitCreate.ro [private]

6.15.4.3 sk_share

BigInteger at.iaik.mpc_acc.MPC_WitCreate.sk_share [private]

6.15.4.4 x

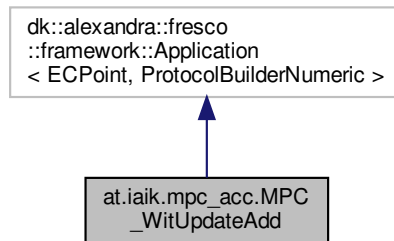
BigInteger at.iaik.mpc_acc.MPC_WitCreate.x [private]

The documentation for this class was generated from the following file:

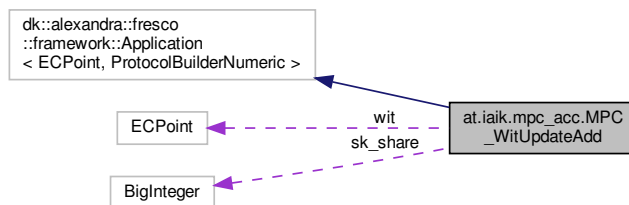
- [MPC_WitCreate.java](#)

6.16 at.iaik.mpc_acc.MPC_WitUpdateAdd Class Reference

Inheritance diagram for at.iaik.mpc_acc.MPC_WitUpdateAdd:



Collaboration diagram for at.iaik.mpc_acc.MPC_WitUpdateAdd:



Public Member Functions

- `MPC_WitUpdateAdd` (BigInteger `sk_share`, ECPoint `wit`)
- `DRes< ECPoint > buildComputation` (ProtocolBuilderNumeric producer)

Private Attributes

- BigInteger `sk_share`
- ECPoint `wit`

6.16.1 Detailed Description

Implements the functionality to update a witness after an element is added to the accumulator

Author

Roman Walch

6.16.2 Constructor & Destructor Documentation

6.16.2.1 MPC_WitUpdateAdd()

```
at.iaik.mpc_acc.MPC_WitUpdateAdd.MPC_WitUpdateAdd (
    BigInteger sk_share,
    ECPoint wit )
```

Construct a witness update computation object for element addition

Parameters

<i>sk_share</i>	the shared secret key
<i>x</i>	the added element
<i>wit</i>	the witness to be updated

6.16.3 Member Function Documentation

6.16.3.1 buildComputation()

```
DRes<ECPoint> at.iaik.mpc_acc.MPC_WitUpdateAdd.buildComputation (
    ProtocolBuilderNumeric producer )
```

Performs the MPC computation to update a witness after an element is added to the accumulator

Returns

the updated witness

Generated by Doxygen

6.16.4 Member Data Documentation

6.16.4.1 sk_share

BigInteger at.iaik.mpc_acc.MPC_WitUpdateAdd.sk_share [private]

6.16.4.2 wit

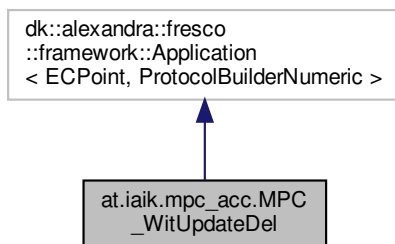
ECPoint at.iaik.mpc_acc.MPC_WitUpdateAdd.wit [private]

The documentation for this class was generated from the following file:

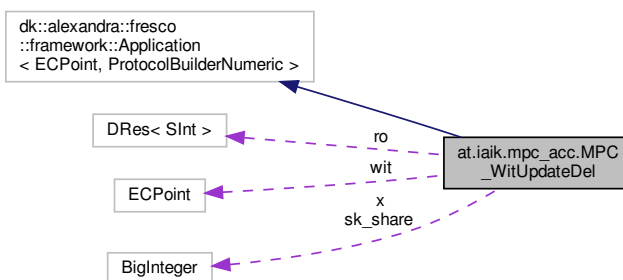
- [MPC_WitUpdateAdd.java](#)

6.17 at.iaik.mpc_acc.MPC_WitUpdateDel Class Reference

Inheritance diagram for at.iaik.mpc_acc.MPC_WitUpdateDel:



Collaboration diagram for at.iaik.mpc_acc.MPC_WitUpdateDel:



Public Member Functions

- `MPC_WitUpdateDel` (`BigInteger sk_share`, `BigInteger x`, `ECPoint wit`)
- `DRes< ECPoint > buildComputation` (`ProtocolBuilderNumeric producer`)

Private Attributes

- `BigInteger sk_share`
- `BigInteger x`
- `ECPoint wit`
- `DRes< Sint > ro`

6.17.1 Detailed Description

Implements the functionality to update a witness after an element is removed from the accumulator

Author

Roman Walch

6.17.2 Constructor & Destructor Documentation**6.17.2.1 MPC_WitUpdateDel()**

```
at.iaik.mpc_acc.MPC_WitUpdateDel.MPC_WitUpdateDel (
    BigInteger sk_share,
    BigInteger x,
    ECPoint wit )
```

Construct a witness update computation object for element removal

Parameters

<i>sk_share</i>	the shared secret key
<i>x</i>	the removed element
<i>wit</i>	the witness to be updated

6.17.3 Member Function Documentation**6.17.3.1 buildComputation()**

```
DRes<ECPoint> at.iaik.mpc_acc.MPC_WitUpdateDel.buildComputation (
    ProtocolBuilderNumeric producer )
```

Performs the MPC computation to update a witness after an element is removed from the accumulator

Generated by Doxygen

Returns

the updated witness

6.17.4 Member Data Documentation

6.17.4.1 ro

DRes<SInt> at.iaik.mpc_acc.MPC_WitUpdateDel.ro [private]

6.17.4.2 sk_share

BigInteger at.iaik.mpc_acc.MPC_WitUpdateDel.sk_share [private]

6.17.4.3 wit

ECPoint at.iaik.mpc_acc.MPC_WitUpdateDel.wit [private]

6.17.4.4 x

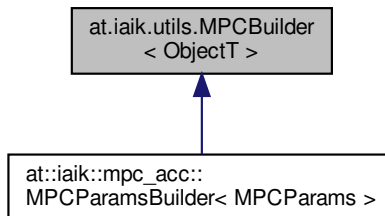
BigInteger at.iaik.mpc_acc.MPC_WitUpdateDel.x [private]

The documentation for this class was generated from the following file:

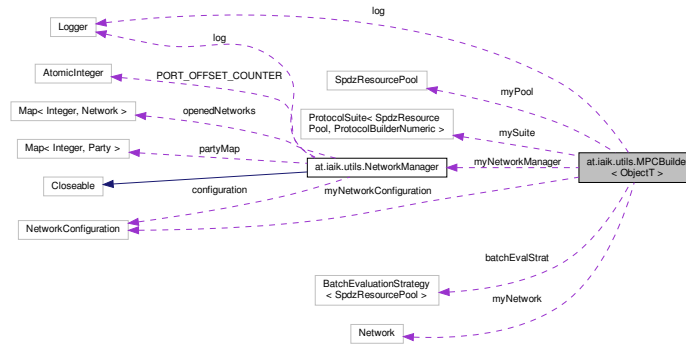
- [MPC_WitUpdateDel.java](#)

6.18 at.iaik.utils.MPCBuilder< ObjectT > Class Template Reference

Inheritance diagram for at.iaik.utils.MPCBuilder< ObjectT >:



Collaboration diagram for at.iaik.util.MPCBuilder< ObjectT > :



Public Member Functions

- `MPCBuilder` (boolean `logging`)
- `MPCBuilder< ObjectT > withID` (int `id`)
- `MPCBuilder< ObjectT > withResourcePool` (PreprocessingStrategy `strategy`, BigInteger `modulus`) throws `ParseException`
- `MPCBuilder< ObjectT > withSpdzLength` (int `maxBitLength`)
- `MPCBuilder< ObjectT > withBatchEvalStrat` (EvaluationStrategy `strat`)
- `MPCBuilder< ObjectT > withNetwork` (Map< Integer, Party > `parties`, Party `myParty`) throws `ParseException`
- abstract `ObjectT build` ()

Static Protected Member Functions

- static `Drbg getDrbg` (int `myId`, int `prgSeedLength`)
- static `SpdzSInt [] computeSInts` (DRes< List< DRes< SInt >>> `pipe`)
- static `DRes< List< DRes< SInt >>> createPipe` (int `myId`, int `noOfPlayers`, int `pipeLength`, Network `pipeNetwork`, SpdzMascotDataSupplier `tripleSupplier`, int `maxBitLength`)
- static void `evaluate` (ProtocolBuilderNumeric `spdzBuilder`, SpdzResourcePool `tripleResourcePool`, Network `network`, SpdzProtocolSuite `spdzProtocolSuite`)
- static `Map< Integer, RotList > getSeedOts` (int `myId`, List< Integer > `partyIds`, int `prgSeedLength`, Drbg `drbg`, Network `network`)

Protected Attributes

- int `numberOfParties`
- int `myID`
- SpdzResourcePool `myPool`
- ProtocolSuite< SpdzResourcePool, ProtocolBuilderNumeric > `mySuite`
- NetworkConfiguration `myNetworkConfiguration`
- BatchEvaluationStrategy< SpdzResourcePool > `batchEvalStrat`
- Network `myNetwork`
- int `maxBitLength`
- NetworkManager `myNetworkManager`
- Logger `log` = `LoggerFactory.getLogger(MPCBuilder.class)`
- boolean `logging`

Generated by Doxygen

6.18.1 Detailed Description

The abstract builder class to instantiate the application objects. This builder takes care of the boiler plate code which is required to setup the framework. It also handles the use case specific input, these two parts could be separated at some point..

Parameters

<ObjectT>	The Object type the Builder extension wants to implement (either client or host)
-----------	--

Author

Fabian Schmid

6.18.2 Constructor & Destructor Documentation

6.18.2.1 MPCBuilder()

```
at.iaik.utils.MPCBuilder< ObjectT >.MPCBuilder (
    boolean logging )
```

Creating the builder following the builder pattern.

Parameters

<i>logging</i>	whether logging is activated during the computation
----------------	---

6.18.3 Member Function Documentation

6.18.3.1 build()

```
abstract ObjectT at.iaik.utils.MPCBuilder< ObjectT >.build ( ) [abstract]
```

This function has to be implemented in each child

Returns

The Object of the class which is built here

6.18.3.2 computeSInts()

```
static SpdzSInt [] at.iaik.utils.MPCBuilder< ObjectT >.computeSInts (
    DRes< List< DRes< SInt >>> pipe ) [static], [protected]
```

Converting the List of SInts that the are the pipe into an array of SpdzSInts

Parameters

<i>pipe</i>	the pipe to be converted
-------------	--------------------------

Returns

the array of SpdzSInt

6.18.3.3 createPipe()

```
static DRes<List<DRes<SInt> > > at.iaik.utils.MPCBuilder< ObjectT >.createPipe (
    int myId,
    int noOfPlayers,
    int pipeLength,
    Network pipeNetwork,
    SpdzMascotDataSupplier tripleSupplier,
    int maxBitLength ) [static], [protected]
```

Creates a protocol for the exponentiation pipe.

Parameters

<i>myId</i>	my id
<i>noOfPlayers</i>	the number of players in the network
<i>pipeLength</i>	the required length of the new pipe
<i>pipeNetwork</i>	the network to be used to create the network in an MPC environment
<i>tripleSupplier</i>	A simple triple supplier used to do the pipe creation using the MASCOT protocol
<i>maxBitLength</i>	the maximum bit length of variables in this application

Returns

The newly created pipe

6.18.3.4 evaluate()

```
static void at.iaik.utils.MPCBuilder< ObjectT >.evaluate (
    ProtocolBuilderNumeric spdzBuilder,
    SpdzResourcePool tripleResourcePool,
    Network network,
    SpdzProtocolSuite spdzProtocolSuite ) [static], [protected]
```

Evaluating the pipe creation protocol, so that the deferred pipe can be used

Parameters

<i>spdzBuilder</i>	the protocolbuilder used to do MPC operations
<i>tripleResourcePool</i>	The resource pool used to execute this MPC protocol
<i>network</i>	The network used for communication
<i>spdzProtocolSuite</i>	the protocolSuite instance used

Generated by Doxygen

6.18.3.5 getDrbg()

```
static Drbg at.iaik.utils.MPCBuilder< ObjectT >.getDrbg (
    int myId,
    int prgSeedLength ) [static], [protected]
```

Auxiliary function when initiating the MASCOT protocol in the resource pool function

Parameters

<i>myId</i>	my id
<i>prgSeedLength</i>	the seed length for the deterministic random bit generator

Returns

a new Drbg instance

6.18.3.6 getSeedOts()

```
static Map<Integer, RotList> at.iaik.utils.MPCBuilder< ObjectT >.getSeedOts (
    int myId,
    List< Integer > partyIds,
    int prgSeedLength,
    Drbg drbg,
    Network network ) [static], [protected]
```

An auxiliary function used for the oblivious transfer necessary to initiate the MASCOT protocol.

Parameters

<i>myId</i>	my id
<i>partyIds</i>	a list of all ids in the network
<i>prgSeedLength</i>	the length of the random seed
<i>drbg</i>	the actual random bit generator instance
<i>network</i>	the network used to do the oblivious transfer

Returns

The map of SeedOts

6.18.3.7 withBatchEvalStrat()

```
MPCBuilder<ObjectT> at.iaik.utils.MPCBuilder< ObjectT >.withBatchEvalStrat (
    EvaluationStrategy strat )
```

Set the BatchEvaluationStrategy accordingly, get the loggingDecorator if logging is activated

Parameters

<i>strat</i>	the evaluation strategy to be used
--------------	------------------------------------

Returns

this

6.18.3.8 withID()

```
MPCBuilder<ObjectT> at.iaik.utils.MPCBuilder< ObjectT >.withID (
    int id )
```

Setting the id of the application object

Parameters

<i>id</i>	the id to be set
-----------	------------------

Returns

this

6.18.3.9 withNetwork()

```
MPCBuilder<ObjectT> at.iaik.utils.MPCBuilder< ObjectT >.withNetwork (
    Map< Integer, Party > parties,
    Party myParty ) throws ParseException
```

Setting up a network manager and creating the first network to communicate with the other parties

Parameters

<i>parties</i>	the parties to connect with
<i>myParty</i>	this party

Returns

this

Exceptions

<i>ParseException</i>	is thrown, if myParty is not contained in the map of parties
-----------------------	--

6.18.3.10 `withResourcePool()`

```
MPCBuilder<ObjectT> at.iaik.utils.MPCBuilder< ObjectT >.withResourcePool (
    PreprocessingStrategy strategy,
    BigInteger modulus ) throws ParseException
```

Initializing the resourcePool Object required by the framework. MASCOT has to be used as a preprocessingStrategy to achieve active security

Parameters

<code>strategy</code>	the PreprocessingStrategy used
<code>modBitLength</code>	the bitLength of the modulus (128 bit is recommended)

Returns

this

Exceptions

<code>ParseException</code>	thrown when preprocessingStrategy is unknown
-----------------------------	--

6.18.3.11 `withSpdzLength()`

```
MPCBuilder<ObjectT> at.iaik.utils.MPCBuilder< ObjectT >.withSpdzLength (
    int maxBitLength )
```

Instantiating the SpdzProtocolSuite required for the computation

Parameters

<code>maxBitLength</code>	the maximum number of bits for each shared variable
---------------------------	---

Returns

this.

6.18.4 Member Data Documentation

6.18.4.1 `batchEvalStrat`

```
BatchEvaluationStrategy<SpdzResourcePool> at.iaik.utils.MPCBuilder< ObjectT >.batchEvalStrat
[protected]
```

6.18.4.2 log

Logger [at.iaik.utils.MPCBuilder< ObjectT >.log](#) = LoggerFactory.getLogger(MPCBuilder.class)
[protected]

6.18.4.3 logging

boolean [at.iaik.utils.MPCBuilder< ObjectT >.logging](#) [protected]

6.18.4.4 maxBitLength

int [at.iaik.utils.MPCBuilder< ObjectT >.maxBitLength](#) [protected]

6.18.4.5 myID

int [at.iaik.utils.MPCBuilder< ObjectT >.myID](#) [protected]

6.18.4.6 myNetwork

Network [at.iaik.utils.MPCBuilder< ObjectT >.myNetwork](#) [protected]

6.18.4.7 myNetworkConfiguration

NetworkConfiguration [at.iaik.utils.MPCBuilder< ObjectT >.myNetworkConfiguration](#) [protected]

6.18.4.8 myNetworkManager

NetworkManager [at.iaik.utils.MPCBuilder< ObjectT >.myNetworkManager](#) [protected]

6.18.4.9 myPool

SpdzResourcePool [at.iaik.utils.MPCBuilder< ObjectT >.myPool](#) [protected]

6.18.4.10 mySuite

ProtocolSuite<SpdzResourcePool, ProtocolBuilderNumeric> [at.iaik.utils.MPCBuilder](#)< ObjectT >.mySuite [protected]

6.18.4.11 numberOfParties

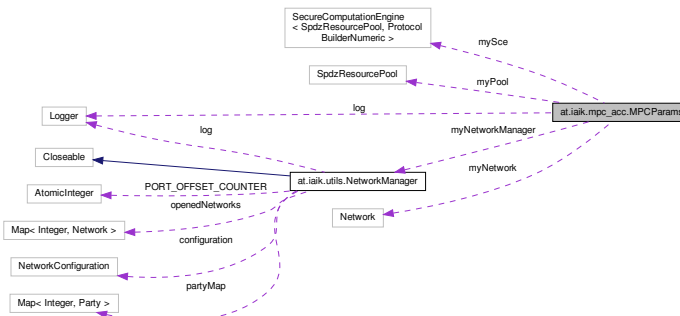
int [at.iaik.utils.MPCBuilder](#)< ObjectT >.numberOfParties [protected]

The documentation for this class was generated from the following file:

- [MPCBuilder.java](#)

6.19 at.iaik.mpc_acc.MPCParams Class Reference

Collaboration diagram for at.iaik.mpc_acc.MPCParams:



Public Member Functions

- [NetworkManager](#) `getMyNetworkManager` ()
- boolean `isLogging` ()
- [Network](#) `getMyNetwork` ()
- [SpdzResourcePool](#) `getMyPool` ()
- [SecureComputationEngine](#)< [SpdzResourcePool](#), [ProtocolBuilderNumeric](#) > `getMySce` ()
- void `closeNetwork` ()
- void `shutdownSce` ()
- void `shutdown` ()
- void `log` (String string)

6.19.1 Detailed Description

[MPCParams](#) The build computation function adds the MPC functionality to the protocol builder

Author

Fabian Schmid

Generated by Doxygen

6.19.2 Member Function Documentation

6.19.2.1 closeNetwork()

```
void at.iaik.mpc_acc.MPCParams.closeNetwork ( )
```

Closes the network

6.19.2.2 getMyNetwork()

```
Network at.iaik.mpc_acc.MPCParams.getMyNetwork ( )
```

Getter for the network

6.19.2.3 getMyNetworkManager()

```
NetworkManager at.iaik.mpc_acc.MPCParams.getMyNetworkManager ( )
```

Getter for the network manager

6.19.2.4 getMyPool()

```
SpdzResourcePool at.iaik.mpc_acc.MPCParams.getMyPool ( )
```

Getter for the resource pool

6.19.2.5 getMySce()

```
SecureComputationEngine<SpdzResourcePool, ProtocolBuilderNumeric> at.iaik.mpc_acc.MPCParams.↔  
getMySce ( )
```

Getter for the secure computation engine

6.19.2.6 isLogging()

```
boolean at.iaik.mpc_acc.MPCParams.isLogging ( )
```

6.19.2.7 log()

```
void at.iaik.mpc_acc.MPCParams.log (  
    String string )
```

6.19.2.8 shutdown()

```
void at.iaik.mpc_acc.MPCParams.shutdown ( )
```

Closes the network and the secure computation engine.

Generated by Doxygen

6.19.2.9 shutdownSce()

```
void at.iaik.mpc_acc.MPCParams.shutdownSce ( )
```

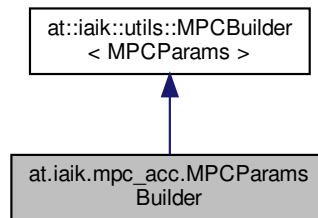
Closes the secure computation engine.

The documentation for this class was generated from the following file:

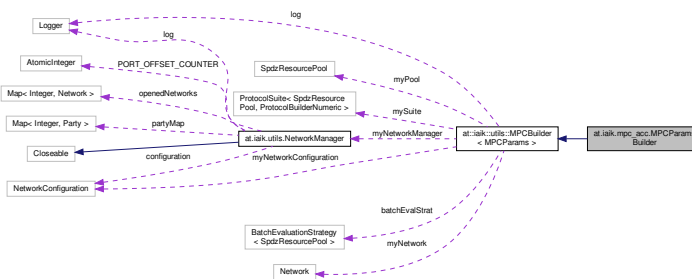
- [MPCParams.java](#)

6.20 at.iaik.mpc_acc.MPCParamsBuilder Class Reference

Inheritance diagram for at.iaik.mpc_acc.MPCParamsBuilder:



Collaboration diagram for at.iaik.mpc_acc.MPCParamsBuilder:



Public Member Functions

- [MPCParamsBuilder](#) (boolean logging)
- [MPCParams build](#) ()

Additional Inherited Members

6.20.1 Detailed Description

[MPCParamsBuilder](#), extends the generic Builder and facilitates creating an instance of the client application: [MP↔CParams](#)

Author

Fabian Schmid

6.20.2 Constructor & Destructor Documentation

6.20.2.1 MPCParamsBuilder()

```
at.iaik.mpc_acc.MPCParamsBuilder.MPCParamsBuilder (
    boolean logging )
```

6.20.3 Member Function Documentation

6.20.3.1 build()

```
MPCParams at.iaik.mpc_acc.MPCParamsBuilder.build ( )
```

The [MPCParams](#) object is created and its members are set according to the members set in the parent builder.

Returns

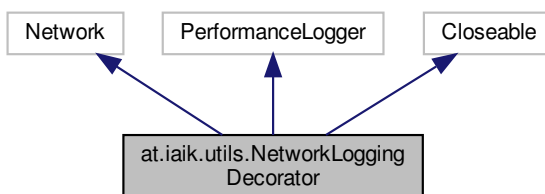
the fully initiated [MPCParams](#) object.

The documentation for this class was generated from the following file:

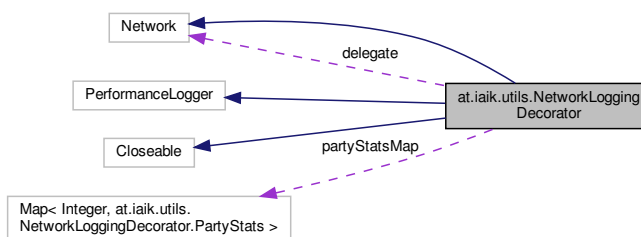
- [MPCParamsBuilder.java](#)

6.21 at.iaik.util.NetworkLoggingDecorator Class Reference

Inheritance diagram for at.iaik.util.NetworkLoggingDecorator:



Collaboration diagram for at.iaik.util.NetworkLoggingDecorator:



Classes

- class [PartyStats](#)

Public Member Functions

- [NetworkLoggingDecorator](#) (Network network)
- `byte [] receive (int partyId)`
- `int getNoOfParties ()`
- `void send (int partyId, byte[] data)`
- `void reset ()`
- `void close ()` throws `IOException`
- `Map< String, Long > getLoggedValues ()`

Static Public Attributes

- static final String `NETWORK_PARTY_BYTES` = "Amount of bytes received pr. party"
- static final String `NETWORK_TOTAL_BYTES` = "Total amount of bytes received"
- static final String `NETWORK_TOTAL_BATCHES` = "Total amount of batches received"

Private Attributes

- Network `delegate`
- Map< Integer, PartyStats > `partyStatsMap` = new HashMap<>()

6.21.1 Detailed Description

A decorator for the network to extract the logged data to the network manager

Author

Fabian Schmid

6.21.2 Constructor & Destructor Documentation**6.21.2.1 NetworkLoggingDecorator()**

```
at.iaik.utils.NetworkLoggingDecorator.NetworkLoggingDecorator (
    Network network )
```

creates the decorator for the given network

Parameters

<code>network</code>	the delegate network to be decorated
----------------------	--------------------------------------

6.21.3 Member Function Documentation**6.21.3.1 close()**

```
void at.iaik.utils.NetworkLoggingDecorator.close ( ) throws IOException
```

6.21.3.2 getLoggedValues()

```
Map<String, Long> at.iaik.utils.NetworkLoggingDecorator.getLoggedValues ( )
```

get the logged values

Returns

Return the entire map of party stats - used in the network Manager

6.21.3.3 getNoOfParties()

```
int at.iaik.utils.NetworkLoggingDecorator.getNoOfParties ( )
```

6.21.3.4 receive()

```
byte [] at.iaik.utils.NetworkLoggingDecorator.receive (
    int partyId )
```

Upon receiving from a party, the received bytes are stored in a map

Parameters

<i>partyId</i>	the party from which to receive
----------------	---------------------------------

Returns

the received bytes

6.21.3.5 reset()

```
void at.iaik.utils.NetworkLoggingDecorator.reset ( )
```

6.21.3.6 send()

```
void at.iaik.utils.NetworkLoggingDecorator.send (
    int partyId,
    byte [] data )
```

6.21.4 Member Data Documentation

6.21.4.1 delegate

```
Network at.iaik.utils.NetworkLoggingDecorator.delegate [private]
```

6.21.4.2 NETWORK_PARTY_BYTES

```
final String at.iaik.utils.NetworkLoggingDecorator.NETWORK_PARTY_BYTES = "Amount of bytes  
received pr. party" [static]
```

6.21.4.3 NETWORK_TOTAL_BATCHES

```
final String at.iaik.utils.NetworkLoggingDecorator.NETWORK_TOTAL_BATCHES = "Total amount of  
batches received" [static]
```

6.21.4.4 NETWORK_TOTAL_BYTES

```
final String at.iaik.utils.NetworkLoggingDecorator.NETWORK_TOTAL_BYTES = "Total amount of  
bytes received" [static]
```

6.21.4.5 partyStatsMap

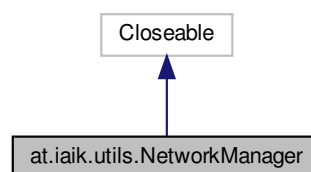
```
Map<Integer, PartyStats> at.iaik.utils.NetworkLoggingDecorator.partyStatsMap = new Hash<↔  
Map<>() [private]
```

The documentation for this class was generated from the following file:

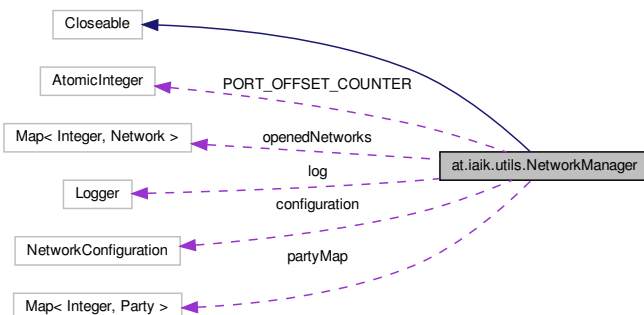
- [NetworkLoggingDecorator.java](#)

6.22 at.iaik.utils.NetworkManager Class Reference

Inheritance diagram for at.iaik.utils.NetworkManager:



Collaboration diagram for at.iaik.utils.NetworkManager:



Public Member Functions

- [NetworkManager](#) ([NetworkConfiguration](#) `configuration`, boolean `logging`, [Map< Integer, Party >](#) `parties`)
- [Network](#) `createExtraNetwork` ()
- [Map< Integer, Party >](#) `getParties` ()
- [Map< String, Long >](#) `getLoggedValues` ()
- void `reset` ()
- void `close` ()

Static Public Member Functions

- static boolean `equalParties` ([Party](#) `p1`, [Party](#) `p2`)
- static [Map< Integer, Party >](#) `getPartyMap` ([List< Map< Integer, Party >>](#) `partyList`, [Party](#) `myParty`)

Private Member Functions

- void `log` ([String](#) `string`)
- [NetworkConfiguration](#) `UpdateConfiguration` ()
- void `close` ([Closeable](#) `closeable`)

Private Attributes

- final [AtomicInteger](#) `PORT_OFFSET_COUNTER` = new [AtomicInteger](#)(0)
- final int `PORT_INCREMENT` = 50
- final [Map< Integer, Network >](#) `openedNetworks`
- final [Map< Integer, Party >](#) `partyMap`
- final [NetworkConfiguration](#) `configuration`
- int `portOffset`
- final boolean `logging`

Static Private Attributes

- static Logger `log` = `LoggerFactory.getLogger(NetworkManager.class)`

6.22.1 Detailed Description

The `NetworkManager` enables multiple networks with the same participants to be managed.

Author

Fabian Schmid

6.22.2 Constructor & Destructor Documentation**6.22.2.1 NetworkManager()**

```
at.iaik.utils.NetworkManager.NetworkManager (
    NetworkConfiguration configuration,
    boolean logging,
    Map< Integer, Party > parties )
```

Create a new `NetworkManager`

Parameters

<i>configuration</i>	the configuration
<i>logging</i>	whether this application uses logging
<i>parties</i>	the parties with which the networks are created

6.22.3 Member Function Documentation**6.22.3.1 close() [1/2]**

```
void at.iaik.utils.NetworkManager.close ( )
```

closes the `networkManager` and all the networks

6.22.3.2 close() [2/2]

```
void at.iaik.utils.NetworkManager.close (
    Closeable closeable ) [private]
```

closes a specific network

Parameters

<i>closeable</i>	the network to be closed
------------------	--------------------------

6.22.3.3 createExtraNetwork()

```
Network at.iaik.utils.NetworkManager.createExtraNetwork ( )
```

Create another network with the same parties but different ports, just to not interfere with the other protocols using the same network.

Returns

the newly created network

6.22.3.4 equalParties()

```
static boolean at.iaik.utils.NetworkManager.equalParties (
    Party p1,
    Party p2 ) [static]
```

Compare two parties with each other

Parameters

<i>p1</i>	party 1
<i>p2</i>	party 2

Returns

is p1 == p2? (true/false)

6.22.3.5 getLoggedValues()

```
Map<String, Long> at.iaik.utils.NetworkManager.getLoggedValues ( )
```

If logging is activated, returns all the logged values from all networks this is used to gather the amount of network traffic received from all the parties

Returns

The string map of all the loggings

6.22.3.6 getParties()

```
Map<Integer, Party> at.iaik.utils.NetworkManager.getParties ( )
```

6.22.3.7 getPartyMap()

```
static Map<Integer, Party> at.iaik.utils.NetworkManager.getPartyMap (
    List< Map< Integer, Party >> partyList,
    Party myParty ) [static]
```

in a multithreaded setting there are several parties with the same id... Returns that party map, which contains my party instance

Parameters

<i>partyList</i>	the list of all party maps
<i>myParty</i>	the instance of my party object

Returns

the party map which this party belongs to

6.22.3.8 log()

```
void at.iaik.utils.NetworkManager.log (
    String string ) [private]
```

6.22.3.9 reset()

```
void at.iaik.utils.NetworkManager.reset ( )
```

6.22.3.10 UpdateConfiguration()

```
NetworkConfiguration at.iaik.utils.NetworkManager.UpdateConfiguration ( ) [private]
```

create new Network configuration by incrementing the ports

Returns

the new network configuration

6.22.4 Member Data Documentation

6.22.4.1 configuration

```
final NetworkConfiguration at.iaik.utils.NetworkManager.configuration [private]
```

6.22.4.2 log

```
Logger at.iaik.utils.NetworkManager.log = LoggerFactory.getLogger(NetworkManager.class) [static],  
[private]
```

6.22.4.3 logging

```
final boolean at.iaik.utils.NetworkManager.logging [private]
```

6.22.4.4 openedNetworks

```
final Map<Integer, Network> at.iaik.utils.NetworkManager.openedNetworks [private]
```

6.22.4.5 partyMap

```
final Map<Integer, Party> at.iaik.utils.NetworkManager.partyMap [private]
```

6.22.4.6 PORT_INCREMENT

```
final int at.iaik.utils.NetworkManager.PORT_INCREMENT = 50 [private]
```

6.22.4.7 PORT_OFFSET_COUNTER

```
final AtomicInteger at.iaik.utils.NetworkManager.PORT_OFFSET_COUNTER = new AtomicInteger(0)  
[private]
```

6.22.4.8 portOffset

```
int at.iaik.utils.NetworkManager.portOffset [private]
```

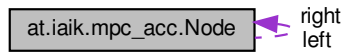
The documentation for this class was generated from the following file:

- [NetworkManager.java](#)

Generated by Doxygen

6.23 at.iaik.mpc_acc.Node Class Reference

Collaboration diagram for at.iaik.mpc_acc.Node:



Public Member Functions

- [Node](#) (byte[] *digest*)
- [Node](#) ([Node left](#), [Node right](#))
- void [compute_digest](#) ()

Static Public Member Functions

- static byte [] [compute_digest](#) (byte[] *left*, byte[] *right*)

Public Attributes

- byte [] [digest](#)
- [Node left](#)
- [Node right](#)

6.23.1 Detailed Description

A class containing the node of a Merkle Tree accumulator

Author

Roman Walch

6.23.2 Constructor & Destructor Documentation

6.23.2.1 [Node\(\)](#) [1/2]

```
at.iaik.mpc_acc.Node.Node (
    byte [] digest )
```

Initialize a node without child-nodes

Parameters

<i>digest</i>	the digest of the node
---------------	------------------------

6.23.2.2 Node() [2/2]

```
at.iaik.mpc_acc.Node.Node (
    Node left,
    Node right )
```

Initialize a node with two child nodes

Parameters

<i>left</i>	the left child
<i>right</i>	the right child

6.23.3 Member Function Documentation

6.23.3.1 compute_digest() [1/2]

```
void at.iaik.mpc_acc.Node.compute_digest ( )
```

Computes the digest of the node.

6.23.3.2 compute_digest() [2/2]

```
static byte [] at.iaik.mpc_acc.Node.compute_digest (
    byte [] left,
    byte [] right ) [static]
```

computes the digest of the node.

Parameters

<i>left</i>	the left child node digest
<i>right</i>	the right child node digest

Returns

the digest of the node

6.23.4 Member Data Documentation

6.23.4.1 digest

byte [] at.iaik.mpc_acc.Node.digest

6.23.4.2 left

Node at.iaik.mpc_acc.Node.left

6.23.4.3 right

Node at.iaik.mpc_acc.Node.right

The documentation for this class was generated from the following file:

- [Node.java](#)

6.24 at.iaik.utils.NetworkLoggingDecorator.PartyStats Class Reference

Public Member Functions

- void [recordTransmission](#) (int noBytes)

Private Attributes

- long [count](#)
- long [noBytes](#)

6.24.1 Detailed Description

The data structure to store information about received transmissions

6.24.2 Member Function Documentation

6.24.2.1 recordTransmission()

```
void at.iaik.utils.NetworkLoggingDecorator.PartyStats.recordTransmission (  
    int noBytes )
```

Upon receiving information, record transmission is called

Parameters

<i>noBytes</i>	the number of bytes received
----------------	------------------------------

6.24.3 Member Data Documentation

6.24.3.1 count

```
long at.iaik.utils.NetworkLoggingDecorator.PartyStats.count [private]
```

6.24.3.2 noBytes

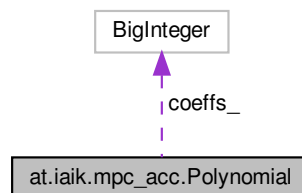
```
long at.iaik.utils.NetworkLoggingDecorator.PartyStats.noBytes [private]
```

The documentation for this class was generated from the following file:

- [NetworkLoggingDecorator.java](#)

6.25 at.iaik.mpc_acc.Polynomial Class Reference

Collaboration diagram for at.iaik.mpc_acc.Polynomial:



Public Member Functions

- [Polynomial](#) (int degree, BigInteger order)
- int [powX](#) (int currentDegree)
- String [toString](#) ()

Static Public Member Functions

- static [Polynomial expand](#) (BigInteger[] roots, BigInteger order)

Private Attributes

- final BigInteger [] [coeffs_](#)
- final int [degree_](#)

6.25.1 Detailed Description

This class represents a monic, reducible polynomial over Z_p

Author

david
chanser

6.25.2 Constructor & Destructor Documentation

6.25.2.1 Polynomial()

```
at.iaik.mpc_acc.Polynomial.Polynomial (
    int degree,
    BigInteger order )
```

c'tor

Parameters

<i>degree</i>	the degree of the polynomial
<i>order</i>	the order to be applied to the coefficients

6.25.3 Member Function Documentation

6.25.3.1 expand()

```
static Polynomial at.iaik.mpc_acc.Polynomial.expand (
    BigInteger [] roots,
    BigInteger order ) [static]
```

Expands a polynomial of the form $X^{i=0} \{n\} (X + A_i)$

Parameters

<i>roots</i>	The list containing the root A _i
<i>order</i>	modulus

Returns

The expanded polynomial

6.25.3.2 powX()

```
int at.iaik.mpc_acc.Polynomial.powX (
    int currentDegree )
```

Increases the degree_ of the polynomial by 1. This method is immutable.

Parameters

<i>currentDegree</i>	the current degree_
----------------------	------------------------

Returns

the resulting polynomial

6.25.3.3 toString()

```
String at.iaik.mpc_acc.Polynomial.toString ( )
```

6.25.4 Member Data Documentation

6.25.4.1 coeffs_

```
final BigInteger [] at.iaik.mpc_acc.Polynomial.coeffs_ [private]
```

6.25.4.2 degree_

```
final int at.iaik.mpc_acc.Polynomial.degree_ [private]
```

The documentation for this class was generated from the following file:

- [Polynomial.java](#)

Generated by Doxygen

6.26 at.iaik.mpc_acc.MerkleTree.Position Enum Reference

89

6.26 at.iaik.mpc_acc.MerkleTree.Position Enum Reference

Public Attributes

- [left](#)
- [right](#)

6.26.1 Detailed Description

Enum for the position of the node as part of the proof.

6.26.2 Member Data Documentation

6.26.2.1 left

`at.iaik.mpc_acc.MerkleTree.Position.left`

6.26.2.2 right

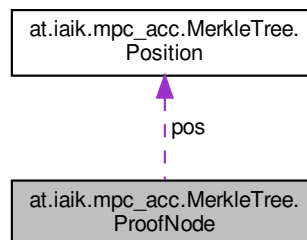
`at.iaik.mpc_acc.MerkleTree.Position.right`

The documentation for this enum was generated from the following file:

- [MerkleTree.java](#)

6.27 at.iaik.mpc_acc.MerkleTree.ProofNode Class Reference

Collaboration diagram for at.iaik.mpc_acc.MerkleTree.ProofNode:



Public Member Functions

- [ProofNode](#) (byte[] *digest*, [Position](#) *pos*)

Public Attributes

- byte [] [digest](#)
- [Position](#) *pos*

6.27.1 Constructor & Destructor Documentation

6.27.1.1 ProofNode()

```
at.iaik.mpc_acc.MerkleTree.ProofNode.ProofNode (  
    byte [] digest,  
    Position pos )
```

6.27.2 Member Data Documentation

6.27.2.1 digest

```
byte [] at.iaik.mpc_acc.MerkleTree.ProofNode.digest
```

6.27.2.2 pos

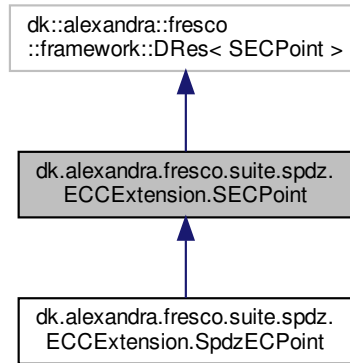
```
Position at.iaik.mpc_acc.MerkleTree.ProofNode.pos
```

The documentation for this class was generated from the following file:

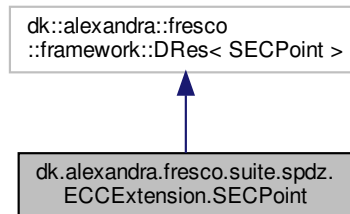
- [MerkleTree.java](#)

6.28 dk.alexandra.fresco.suite.spdz.ECCEExtension.SECPoint Interface Reference

Inheritance diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SECPoint:



Collaboration diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SECPoint:



6.28.1 Detailed Description

A interface class to make the Secure Elliptic Curve Point usable by FRESKO's applications

Author

Roman Walch

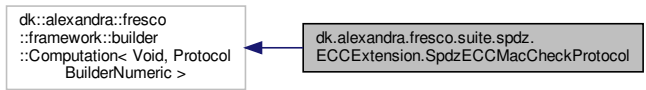
The documentation for this interface was generated from the following file:

- [SECPoint.java](#)

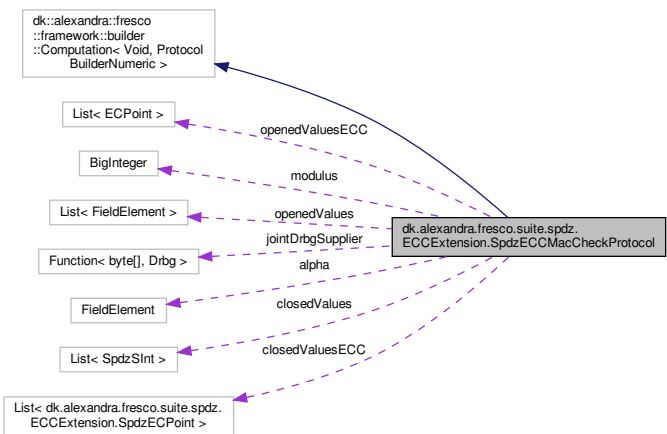
Generated by Doxygen

6.29 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol Class Reference

Inheritance diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol:



Collaboration diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol:



Public Member Functions

- [SpdzECCMacCheckProtocol](#) (final Pair< List< SpdzSInt >, List< FieldElement >> toCheck, final Pair< List< SpdzECPoint >, List< ECPoint >> toCheckECC, final BigInteger modulus, final Function< byte[], Drbg > jointDrbgSupplier, final FieldElement alpha, final int drbgSeedBitLength)
- DRes< Void > [buildComputation](#) (ProtocolBuilderNumeric builder)

Private Member Functions

- FieldElement [] [sampleRandomCoefficients](#) (int numCoefficients, FieldDefinition fieldDefinition, Drbg joint←→ Drbg)

Private Attributes

- final BigInteger `modulus`
- final List< SpdzSInt > `closedValues`
- final List< FieldElement > `openedValues`
- final List< SpdzECPoint > `closedValuesECC`
- final List< ECPoint > `openedValuesECC`
- final FieldElement `alpha`
- final Function< byte[], Drbg > `jointDrbgSupplier`
- final int `drbgByteLength`

6.29.1 Detailed Description

Protocol which handles the MAC check internal to SPDZ. If this protocol reaches the end, no malicious activity was detected and the storage is reset. This class is an Extension to the SpdzMacCheckProtocol class according to <https://eprint.iacr.org/2019/768>

Author

Roman Walch

6.29.2 Constructor & Destructor Documentation

6.29.2.1 SpdzECCMacCheckProtocol()

```
dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzECCMacCheckProtocol.SpdzECCMacCheckProtocol (
    final Pair< List< SpdzSInt >, List< FieldElement >> toCheck,
    final Pair< List< SpdzECPoint >, List< ECPoint >> toCheckECC,
    final BigInteger modulus,
    final Function< byte[], Drbg > jointDrbgSupplier,
    final FieldElement alpha,
    final int drbgSeedBitLength )
```

A Constructor for ECCMacCheckProtocol. This protocol handles the MAC check internal to SPDZ for ECC Points. If this protocol reaches the end, no malicious activity was detected and the storage is reset.

Parameters

<i>toCheck</i>	opened values and corresponding macs to check
<i>modulus</i>	the global modulus used
<i>jointDrbgSupplier</i>	supplier of DRBG to be used for joint randomness
<i>alpha</i>	this party's key share
<i>drbgSeedBitLength</i>	seed length for local DRBG

6.29.3 Member Function Documentation

6.29.3.1 buildComputation()

```
DRes<Void> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol.buildComputation
(
    ProtocolBuilderNumeric builder )
```

Adds the ECC MacCheck to the execution queue.

Parameters

<i>builder</i>	The builder used to build the computation
----------------	---

6.29.3.2 sampleRandomCoefficients()

```
FieldElement [] dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol.sample↵
RandomCoefficients (
    int numCoefficients,
    FieldDefinition fieldDefinition,
    Drbg jointDrbg ) [private]
```

This member samples the random coefficients used during the MAC check

6.29.4 Member Data Documentation

6.29.4.1 alpha

```
final FieldElement dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol.alpha
[private]
```

this party's key share

6.29.4.2 closedValues

```
final List<SpdzSInt> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol.↵
closedValues [private]
```

List of closed Integers

6.29.4.3 closedValuesECC

```
final List<SpdzECPPoint> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol.↵
closedValuesECC [private]
```

List of closed ECC Points

6.29.4.4 drbgByteLength

```
final int dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol.drbgByteLength
[private]
```

seed length for local DRBG

6.29.4.5 jointDrbgSupplier

```
final Function<byte[], Drbg> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheck↔
Protocol.jointDrbgSupplier [private]
```

supplier of DRBG to be used for joint randomness

6.29.4.6 modulus

```
final BigInteger dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol.modulus
[private]
```

The ECC modulus

6.29.4.7 openedValues

```
final List<FieldElement> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol.↔
openedValues [private]
```

List of opened Integers

6.29.4.8 openedValuesECC

```
final List<ECPoint> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol.↔
openedValuesECC [private]
```

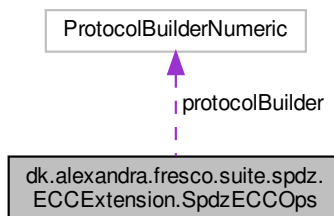
List of opened ECC Points

The documentation for this class was generated from the following file:

- [SpdzECCMacCheckProtocol.java](#)

6.30 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps Class Reference

Collaboration diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps:



Public Member Functions

- [SpdzECCOps](#) (ProtocolBuilderNumeric [protocolBuilder](#))
- DRes< SInt > [knownScalar](#) (BigInteger k)
- DRes< [SECPPoint](#) > [knownMultiply](#) (ECPoint p, BigInteger k)
- DRes< [SECPPoint](#) > [multiply](#) (ECPoint p, DRes< SInt > k)
- DRes< ECPoint > [open](#) (DRes< [SECPPoint](#) > secretshare)

Private Attributes

- final ProtocolBuilderNumeric [protocolBuilder](#)

6.30.1 Detailed Description

A class containing wrappers to append elliptic curve computations to FRESCO's applications

Author

Roman Walch

6.30.2 Constructor & Destructor Documentation**6.30.2.1 SpdzECCOps()**

```
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps.SpdzECCOps (
    ProtocolBuilderNumeric protocolBuilder )
```

The constructor of the class. It sets the used builder

Parameters

<i>protocolBuilder</i>	the used protocol builder
------------------------	---------------------------

6.30.3 Member Function Documentation**6.30.3.1 knownMultiply()**

```
DRes<SECPPoint> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps.knownMultiply (
    ECPoint p,
    BigInteger k )
```

Creates a valid shared integer from a previously shared value (which had no associated MAC) and multiplies it to a public ECC point

Parameters

p	The public ECC point
k	the previous shared value

Returns

the resulting shared ECC point

6.30.3.2 knownScalar()

```
DRes<SInt> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps.knownScalar (
    BigInteger k )
```

Creates a valid shared integer from a previously shared value (which had no associated MAC)

Parameters

k	the previous shared value
-----	---------------------------

Returns

the valid shared integer

6.30.3.3 multiply()

```
DRes<SECPPoint> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps.multiply (
    ECPPoint p,
    DRes< SInt > k )
```

Multiplies a shared integer to an public ECC point

Parameters

p	The public ECC point
k	the shared integer

Returns

the resulting shared ECC point

6.30.3.4 open()

```
DRes<ECPPoint> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps.open (  
    DRes< SECPPoint > secretshare )
```

Opens a shared ECC point

Parameters

<code>secretshare</code>	the shared ECC point
--------------------------	----------------------

Returns

the public opened ECC point

6.30.4 Member Data Documentation

6.30.4.1 protocolBuilder

```
final ProtocolBuilderNumeric dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps.protocolBuilder [private]
```

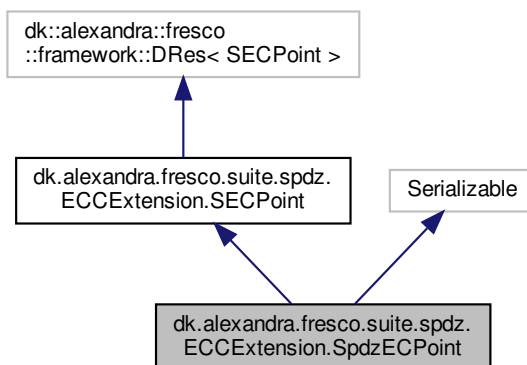
the used protocol builder

The documentation for this class was generated from the following file:

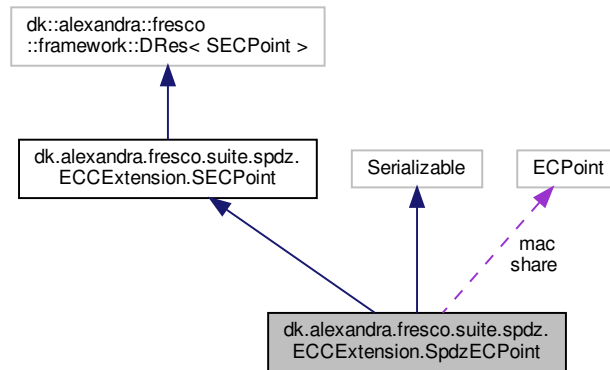
- [SpdzECCOps.java](#)

6.31 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPoint Class Reference

Inheritance diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPoint:



Collaboration diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPPoint:



Public Member Functions

- [SpdzECPPoint](#) (ECPPoint [share](#), ECPPoint [mac](#))
- String [toString](#) ()
- [SECPPoint](#) [out](#) ()
- ECPPoint [getShare](#) ()
- ECPPoint [getMac](#) ()
- byte [] [serializeShare](#) ()
- EllipticCurve [getCurve](#) ()

Static Public Member Functions

- static [SpdzECPPoint multiplyPoint](#) (ECPPoint [p](#), BigInteger [share](#), BigInteger [mac](#))

Private Attributes

- final ECPPoint [share](#)
- final ECPPoint [mac](#)

Static Private Attributes

- static final long [serialVersionUID](#) = 5882876872861854360L

6.31.1 Detailed Description

A Spdz class for shared ECC points containing the MAC and share.

Author

Roman Walch

6.31.2 Constructor & Destructor Documentation

6.31.2.1 SpdzECPublic()

```
dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzECPublic.SpdzECPublic (
    ECPublic share,
    ECPublic mac )
```

Constructor to initialize the shared ECC point.

Parameters

<i>share</i>	the ECC share
<i>mac</i>	the MAC

6.31.3 Member Function Documentation

6.31.3.1 getCurve()

```
EllipticCurve dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzECPublic.getCurve ( )
```

Returns the curve of the shared ECC point

Returns

the used elliptic curve

6.31.3.2 getMac()

```
ECPublic dk.alexandra.fresco.suite.spdz.ECCExtension.SpdzECPublic.getMac ( )
```

Getter for the MAC

Returns

the MAC

6.31.3.3 getShare()

```
ECPoint dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPPoint.getShare ( )
```

Getter for the share

Returns

the share

6.31.3.4 multiplyPoint()

```
static SpdzECPPoint dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPPoint.multiplyPoint (
    ECPoint p,
    BigInteger share,
    BigInteger mac ) [static]
```

Multiplies a shared integer to an public ECC point

Parameters

<i>p</i>	the public ECC point
<i>share</i>	the share of the shared integer
<i>mac</i>	the MAC of the shared integer

Returns

the resulting shared ECC point

6.31.3.5 out()

```
SECPPoint dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPPoint.out ( )
```

Helper class to output the actual shared ECC point

6.31.3.6 serializeShare()

```
byte [] dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPPoint.serializeShare ( )
```

Serializes the shared ECC point

Returns

the serialization

6.31.3.7 toString()

```
String dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPPoint.toString ( )
```

Covnerts the shared ECC point to a string

6.31.4 Member Data Documentation

6.31.4.1 mac

```
final ECPPoint dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPPoint.mac [private]
```

The corresponding MAC

6.31.4.2 serialVersionUID

```
final long dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPPoint.serialVersionUID = 588287687286185 [static], [private]
```

6.31.4.3 share

```
final ECPPoint dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPPoint.share [private]
```

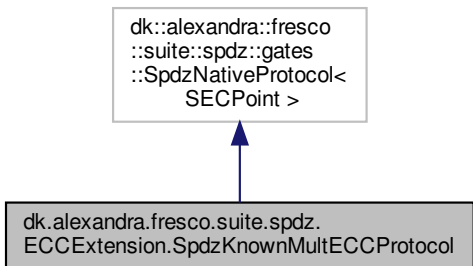
The share of the point

The documentation for this class was generated from the following file:

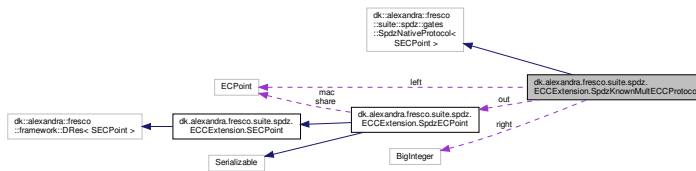
- [SpdzECPPoint.java](#)

6.32 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol Class Reference

Inheritance diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol:



Collaboration diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol:



Public Member Functions

- SpdzKnownMultECCProtocol (ECPoint p, BigInteger k)
- EvaluationStatus evaluate (int round, SpdzResourcePool spdzResourcePool, Network network)
- SpdzECPoint out ()

Private Attributes

- ECPoint left
- BigInteger right
- SpdzECPoint out

6.32.1 Detailed Description

A Spdz protocol to create a valid shared integer from a previously shared value (which had no associated MAC) and multiplies it to a public ECC point

Author

Roman Walch

6.32.2 Constructor & Destructor Documentation

6.32.2.1 SpdzKnownMultECCProtocol()

```
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol.SpdzKnownMultECCProtocol
(
    ECPoint p,
    BigInteger k )
```

The constructor to initialize the computation.

Parameters

<i>p</i>	the public ECC point
<i>k</i>	the previous shared value

Generated by Doxygen

6.32.3 Member Function Documentation

6.32.3.1 evaluate()

```
EvaluationStatus dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol.evaluate  
(  
    int round,  
    SpdzResourcePool spdzResourcePool,  
    Network network )
```

This members shares the previously shared value and multiplies the result to a public ECC point. FRESCO calls this member when executing the SpdzKnownMultECC computation.

6.32.3.2 out()

```
SpdzECPPoint dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol.out ( )
```

Helper class to output the resulting shared ECC point

6.32.4 Member Data Documentation

6.32.4.1 left

```
ECPPoint dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol.left [private]
```

the ECC point.

6.32.4.2 out

```
SpdzECPPoint dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol.out [private]
```

the resulting shared ECC point

6.32.4.3 right

```
BigInteger dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol.right [private]
```

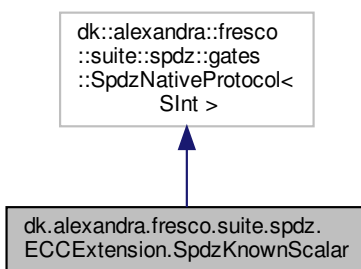
the previously shared Integer

The documentation for this class was generated from the following file:

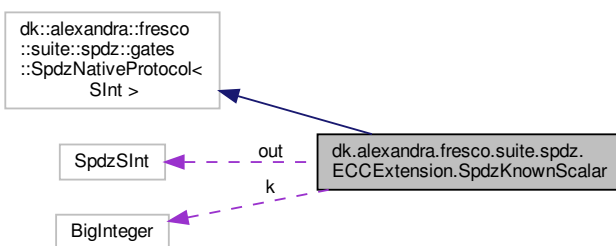
- [SpdzKnownMultECCProtocol.java](#)

6.33 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar Class Reference

Inheritance diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar:



Collaboration diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar:



Public Member Functions

- [SpdzKnownScalar](#) (BigInteger k)
- EvaluationStatus [evaluate](#) (int round, SpdzResourcePool spdzResourcePool, Network network)
- SInt [out](#) ()

Private Attributes

- BigInteger k
- SpdzSInt out

6.33.1 Detailed Description

A Spdz protocol to create a valid shared integer from a previously shared value (which had no associated MAC)

Author

Roman Walch

6.33.2 Constructor & Destructor Documentation

6.33.2.1 SpdzKnownScalar()

```
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar.SpdzKnownScalar (
    BigInteger k )
```

The constructor to initialize the computation.

Parameters

k	the previous shared value
-----	---------------------------

6.33.3 Member Function Documentation

6.33.3.1 evaluate()

```
EvaluationStatus dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar.evaluate (
    int round,
    SpdzResourcePool spdzResourcePool,
    Network network )
```

This members shares the previously shared value. FRESCO calls this member when executing the [SpdzKnown↔Scalar](#) computation.

6.33.3.2 out()

```
SInt dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar.out ( )
```

Helper class to output the resulting shared Integer

6.33.4 Member Data Documentation

6.33.4.1 k

BigInteger dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar.k [private]

the previous shared value

6.33.4.2 out

SpdzSInt dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar.out [private]

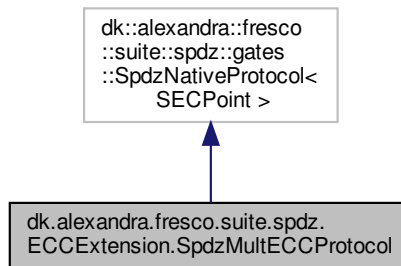
the resulting shared ECC point

The documentation for this class was generated from the following file:

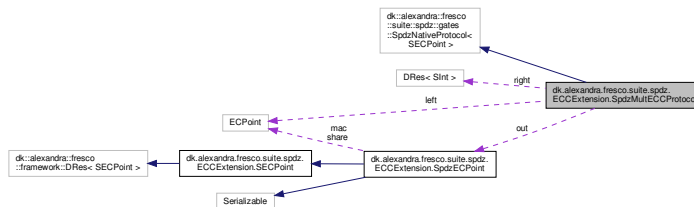
- [SpdzKnownScalar.java](#)

6.34 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol Class Reference

Inheritance diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol:



Collaboration diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol:



Public Member Functions

- [SpdzMultECCProtocol](#) (ECPoint *p*, DRes< SInt > *k*)
- EvaluationStatus [evaluate](#) (int *round*, SpdzResourcePool *spdzResourcePool*, Network *network*)
- [SpdzECPoint out](#) ()

Private Attributes

- ECPoint [left](#)
- DRes< SInt > [right](#)
- [SpdzECPoint out](#)

6.34.1 Detailed Description

A Spdz protocol to multiply a shared integer to an public ECC point.

Author

Roman Walch

6.34.2 Constructor & Destructor Documentation**6.34.2.1 SpdzMultECCProtocol()**

```
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol.SpdzMultECCProtocol (
    ECPoint p,
    DRes< SInt > k )
```

The constructor to initialize the computation.

Parameters

<i>p</i>	the public ECC point
<i>k</i>	the shared integer

6.34.3 Member Function Documentation**6.34.3.1 evaluate()**

```
EvaluationStatus dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol.evaluate (
    int round,
    SpdzResourcePool spdzResourcePool,
    Network network )
```

This member multiplies a shared integer to an public ECC point. FRESCO calls this member when executing the SpdzMultECC computation.

Generated by Doxygen

6.35 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOpenedValueECCStoreImpl Class Reference 110

6.34.3.2 out()

`SpdzECPPoint` dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol.out ()

Helper class to output the resulting shared ECC point

6.34.4 Member Data Documentation

6.34.4.1 left

`ECPPoint` dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol.left [private]

the public ECC point

6.34.4.2 out

`SpdzECPPoint` dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol.out [private]

the resulting shared ECC point

6.34.4.3 right

`DRes<SInt>` dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol.right [private]

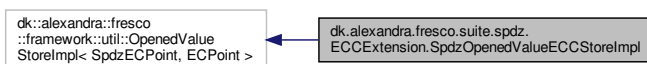
the shared Integer

The documentation for this class was generated from the following file:

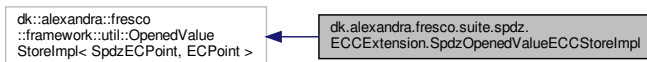
- [SpdzMultECCProtocol.java](#)

6.35 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOpenedValueECCStoreImpl Class Reference

Inheritance diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOpenedValueECCStoreImpl:



Collaboration diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOpenedValueECCStoreImpl:



6.35.1 Detailed Description

Spdz-specific instantiation of OpenedValueStore to store the Opened ECC Values.

Author

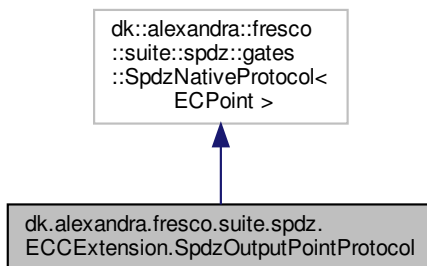
Roman Walch

The documentation for this class was generated from the following file:

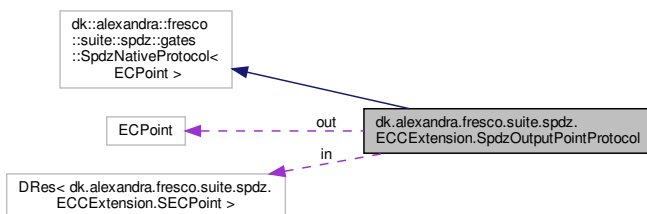
- [SpdzOpenedValueECCStoreImpl.java](#)

6.36 dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOutputPointProtocol Class Reference

Inheritance diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOutputPointProtocol:



Collaboration diagram for dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOutputPointProtocol:



Public Member Functions

- [SpdzOutputPointProtocol](#) (DRes< [SECPPoint](#) > in)
- EvaluationStatus [evaluate](#) (int round, SpdzResourcePool spdzResourcePool, Network network)
- ECPoint [out](#) ()

Private Attributes

- DRes< [SECPPoint](#) > in
- ECPoint [out](#)

6.36.1 Detailed Description

A Spdz protocol to open shared ECC points.

Author

Roman Walch

6.36.2 Constructor & Destructor Documentation**6.36.2.1 SpdzOutputPointProtocol()**

```
dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOutputPointProtocol.SpdzOutputPointProtocol (
    DRes< SECPPoint > in )
```

The constructor to initialize the computation.

Parameters

<i>in</i>	the shared ECC point
-----------	----------------------

6.36.3 Member Function Documentation**6.36.3.1 evaluate()**

```
EvaluationStatus dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOutputPointProtocol.evaluate (
    (
        int round,
        SpdzResourcePool spdzResourcePool,
        Network network )
```

This members opens the the shared ECC point. FRESCO calls this member when executing the SpdzOutputPoint computation.

Generated by Doxygen

6.36.3.2 out()

```
ECPoint dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOutputPointProtocol.out ( )
```

Helper class to output the resulting opened ECC point

6.36.4 Member Data Documentation

6.36.4.1 in

```
DRes<SECPPoint> dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOutputPointProtocol.in [private]
```

the shared ECC point

6.36.4.2 out

```
ECPoint dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOutputPointProtocol.out [private]
```

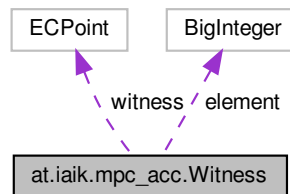
the opened public ECC point

The documentation for this class was generated from the following file:

- [SpdzOutputPointProtocol.java](#)

6.37 at.iaik.mpc_acc.Witness Class Reference

Collaboration diagram for at.iaik.mpc_acc.Witness:



Public Member Functions

- [Witness](#) (ECPoint [witness](#), BigInteger [element](#))
- ECPoint [getWitness](#) ()
- BigInteger [getElement](#) ()

Generated by Doxygen

Private Attributes

- ECPoint [witness](#)
- BigInteger [element](#)

6.37.1 Detailed Description

A simple class containing the [Witness](#) of the [Accumulator](#)

Author

Roman Walch

6.37.2 Constructor & Destructor Documentation**6.37.2.1 Witness()**

```
at.iaik.mpc_acc.Witness.Witness (
    ECPoint witness,
    BigInteger element )
```

A constructor to initialize the [Witness](#) of an element

Parameters

<i>witness</i>	the witness
<i>element</i>	the corresponding element

6.37.3 Member Function Documentation**6.37.3.1 getElement()**

```
BigInteger at.iaik.mpc_acc.Witness.getElement ( )
```

Getter for the corresponding element

Returns

the corresponding element

6.37.3.2 `getWitness()`

```
ECPoint at.iaik.mpc_acc.Witness.getWitness ( )
```

Getter for the witness

Returns

the witness

6.37.4 Member Data Documentation

6.37.4.1 `element`

```
BigInteger at.iaik.mpc_acc.Witness.element [private]
```

6.37.4.2 `witness`

```
ECPoint at.iaik.mpc_acc.Witness.witness [private]
```

The documentation for this class was generated from the following file:

- [Witness.java](#)

7 File Documentation

7.1 Accumulator.java File Reference

Classes

- class [at.iaik.mpc_acc.Accumulator](#)

Packages

- package [at.iaik.mpc_acc](#)

7.2 AccumulatorDemo.java File Reference

Classes

- class [at.iaik.mpc_acc.AccumulatorDemo](#)

7.3 Auxillery.java File Reference

116

Packages

- package [at.iaik.mpc_acc](#)

7.3 Auxillery.java File Reference

Classes

- class [at.iaik.mpc_acc.Auxillery](#)
- enum [at.iaik.mpc_acc.Auxillery.UPDATE](#)

Packages

- package [at.iaik.mpc_acc](#)

7.4 CmdLineParser.java File Reference

Classes

- class [at.iaik.utils.CmdLineParser](#)
- class [at.iaik.utils.CmdLineParser.BuilderParams](#)

Packages

- package [at.iaik.utils](#)

7.5 EvalResult.java File Reference

Classes

- class [at.iaik.mpc_acc.EvalResult](#)

Packages

- package [at.iaik.mpc_acc](#)

7.6 Main.java File Reference

Classes

- class [at.iaik.mpc_acc.Main](#)

Packages

- package [at.iaik.mpc_acc](#)

Generated by Doxygen

7.7 MerkleTree.java File Reference

117

7.7 MerkleTree.java File Reference

Classes

- class [at.iaik.mpc_acc.MerkleTree](#)
- class [at.iaik.mpc_acc.MerkleTree.ProofNode](#)
- enum [at.iaik.mpc_acc.MerkleTree.Position](#)

Packages

- package [at.iaik.mpc_acc](#)

7.8 MPC_Acc.java File Reference

Classes

- class [at.iaik.mpc_acc.MPC_Acc](#)

Packages

- package [at.iaik.mpc_acc](#)

7.9 MPC_Add.java File Reference

Classes

- class [at.iaik.mpc_acc.MPC_Add](#)

Packages

- package [at.iaik.mpc_acc](#)

7.10 MPC_Del.java File Reference

Classes

- class [at.iaik.mpc_acc.MPC_Del](#)

Packages

- package [at.iaik.mpc_acc](#)

7.11 MPC_Eval.java File Reference

Classes

- class [at.iaik.mpc_acc.MPC_Eval](#)

Generated by Doxygen

7.12 MPC_Gen.java File Reference

118

Packages

- package [at.iaik.mpc_acc](#)

7.12 MPC_Gen.java File Reference

Classes

- class [at.iaik.mpc_acc.MPC_Gen](#)

Packages

- package [at.iaik.mpc_acc](#)

7.13 MPC_TripleDummy.java File Reference

Classes

- class [at.iaik.mpc_acc.MPC_TripleDummy](#)

Packages

- package [at.iaik.mpc_acc](#)

7.14 MPC_WitCreate.java File Reference

Classes

- class [at.iaik.mpc_acc.MPC_WitCreate](#)

Packages

- package [at.iaik.mpc_acc](#)

7.15 MPC_WitUpdateAdd.java File Reference

Classes

- class [at.iaik.mpc_acc.MPC_WitUpdateAdd](#)

Packages

- package [at.iaik.mpc_acc](#)

Generated by Doxygen

7.16 MPC_WitUpdateDel.java File Reference

119

7.16 MPC_WitUpdateDel.java File Reference

Classes

- class [at.iaik.mpc_acc.MPC_WitUpdateDel](#)

Packages

- package [at.iaik.mpc_acc](#)

7.17 MPCBuilder.java File Reference

Classes

- class [at.iaik.utils.MPCBuilder](#)< [Object](#)T >

Packages

- package [at.iaik.utils](#)

7.18 MPCParams.java File Reference

Classes

- class [at.iaik.mpc_acc.MPCParams](#)

Packages

- package [at.iaik.mpc_acc](#)

7.19 MPCParamsBuilder.java File Reference

Classes

- class [at.iaik.mpc_acc.MPCParamsBuilder](#)

Packages

- package [at.iaik.mpc_acc](#)

7.20 NetworkLoggingDecorator.java File Reference

Classes

- class [at.iaik.utils.NetworkLoggingDecorator](#)
- class [at.iaik.utils.NetworkLoggingDecorator.PartyStats](#)

Generated by Doxygen

7.21 NetworkManager.java File Reference

120

Packages

- package [at.iaik.utils](#)

7.21 NetworkManager.java File Reference

Classes

- class [at.iaik.utils.NetworkManager](#)

Packages

- package [at.iaik.utils](#)

7.22 Node.java File Reference

Classes

- class [at.iaik.mpc_acc.Node](#)

Packages

- package [at.iaik.mpc_acc](#)

7.23 Polynomial.java File Reference

Classes

- class [at.iaik.mpc_acc.Polynomial](#)

Packages

- package [at.iaik.mpc_acc](#)

7.24 SECPPoint.java File Reference

Classes

- interface [dk.alexandra.fresco.suite.spdz.ECCEExtension.SECPPoint](#)

Packages

- package [dk.alexandra.fresco.suite.spdz.ECCEExtension](#)

Generated by Doxygen

7.25 SpdzECCMacCheckProtocol.java File Reference

121

7.25 SpdzECCMacCheckProtocol.java File Reference

Classes

- class [dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCMacCheckProtocol](#)

Packages

- package [dk.alexandra.fresco.suite.spdz.ECCEExtension](#)

7.26 SpdzECCOps.java File Reference

Classes

- class [dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECCOps](#)

Packages

- package [dk.alexandra.fresco.suite.spdz.ECCEExtension](#)

7.27 SpdzECPPoint.java File Reference

Classes

- class [dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzECPPoint](#)

Packages

- package [dk.alexandra.fresco.suite.spdz.ECCEExtension](#)

7.28 SpdzKnownMultECCProtocol.java File Reference

Classes

- class [dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownMultECCProtocol](#)

Packages

- package [dk.alexandra.fresco.suite.spdz.ECCEExtension](#)

7.29 SpdzKnownScalar.java File Reference

Classes

- class [dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzKnownScalar](#)

Generated by Doxygen

7.30 SpdzMultECCProtocol.java File Reference

122

Packages

- package [dk.alexandra.fresco.suite.spdz.ECCEExtension](#)

7.30 SpdzMultECCProtocol.java File Reference

Classes

- class [dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzMultECCProtocol](#)

Packages

- package [dk.alexandra.fresco.suite.spdz.ECCEExtension](#)

7.31 SpdzOpenedValueECCStoreImpl.java File Reference

Classes

- class [dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOpenedValueECCStoreImpl](#)

Packages

- package [dk.alexandra.fresco.suite.spdz.ECCEExtension](#)

7.32 SpdzOutputPointProtocol.java File Reference

Classes

- class [dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzOutputPointProtocol](#)

Packages

- package [dk.alexandra.fresco.suite.spdz.ECCEExtension](#)

7.33 Witness.java File Reference

Classes

- class [at.iaik.mpc_acc.Witness](#)

Packages

- package [at.iaik.mpc_acc](#)

Generated by Doxygen

Index

acc
 at::iaik::mpc_acc::Auxillery, 23
 at::iaik::mpc_acc::EvalResult, 33
 at::iaik::mpc_acc::MPC_Add, 46
 at::iaik::mpc_acc::MPC_Del, 49
 at::iaik::mpc_acc::MPC_WitCreate, 57
 acc_prime
 at::iaik::mpc_acc::Auxillery, 23
 Accumulator
 at::iaik::mpc_acc::Accumulator, 9
 Accumulator.java, 115
 AccumulatorDemo
 at::iaik::mpc_acc::AccumulatorDemo, 15
 AccumulatorDemo.java, 115
 Add
 at::iaik::mpc_acc::Accumulator, 9
 at::iaik::mpc_acc::AccumulatorDemo, 16
 add
 at::iaik::mpc_acc::MPC_Acc, 40
 alpha
 dk::alexandra::fresco::suite::spdz::ECCExtension↔
 ::SpdzECCMacCheckProtocol, 94
 at, 6
 at.iaik, 6
 at.iaik.mpc_acc, 6
 at.iaik.mpc_acc.Accumulator, 8
 at.iaik.mpc_acc.AccumulatorDemo, 14
 at.iaik.mpc_acc.Auxillery, 20
 at.iaik.mpc_acc.EvalResult, 31
 at.iaik.mpc_acc.MPC_Acc, 39
 at.iaik.mpc_acc.MPC_Add, 45
 at.iaik.mpc_acc.MPC_Del, 47
 at.iaik.mpc_acc.MPC_Eval, 49
 at.iaik.mpc_acc.MPC_Gen, 52
 at.iaik.mpc_acc.MPC_TripleDummy, 54
 at.iaik.mpc_acc.MPC_WitCreate, 56
 at.iaik.mpc_acc.MPC_WitUpdateAdd, 58
 at.iaik.mpc_acc.MPC_WitUpdateDel, 60
 at.iaik.mpc_acc.MPCParams, 70
 at.iaik.mpc_acc.MPCParamsBuilder, 72
 at.iaik.mpc_acc.Main, 33
 at.iaik.mpc_acc.MerkleTree, 35
 at.iaik.mpc_acc.MerkleTree.Position, 89
 at.iaik.mpc_acc.MerkleTree.ProofNode, 89
 at.iaik.mpc_acc.Node, 83
 at.iaik.mpc_acc.Polynomial, 86
 at.iaik.mpc_acc.Witness, 113
 at.iaik.utils, 7
 at.iaik.utils.CmdLineParser, 27
 at.iaik.utils.CmdLineParser.BuilderParams, 24
 at.iaik.utils.MPCBuilder< ObjectT >, 62
 at.iaik.utils.NetworkLoggingDecorator, 74
 at.iaik.utils.NetworkLoggingDecorator.PartyStats, 85
 at.iaik.utils.NetworkManager, 77
 at::iaik::mpc_acc::Accumulator
 Accumulator, 9
 Add, 9
 CURVE1, 13
 CURVE2, 13
 Delete, 10
 Eval, 10
 G1, 13
 G2, 13
 Gen, 11
 getRandomScalar, 11
 getQ, 11
 PAIRING, 13
 pk, 13
 pk2, 13
 Q, 14
 random, 14
 size, 14
 t, 14
 test, 11
 Verify, 12
 WitCreate, 12
 WitUpdate, 12
 at::iaik::mpc_acc::AccumulatorDemo
 AccumulatorDemo, 15
 Add, 16
 CURVE1, 19
 CURVE2, 19
 Delete, 16
 Eval, 16
 G1, 19
 G2, 19
 Gen, 17
 getRandomScalar, 17
 PAIRING, 19
 pk2, 19
 Q, 19
 random, 19
 size, 20
 sk, 20
 test, 17
 Verify, 17
 WitCreate, 18
 WitUpdate, 18
 at::iaik::mpc_acc::Auxillery
 acc, 23
 acc_prime, 23
 Auxillery, 21, 22
 clearUpdate, 22
 getAcc, 22
 getAccPrime, 22
 getList, 22
 getUpdate, 22
 getR, 22
 list, 23
 r, 23

- update, 23
- at::iaik::mpc_acc::EvalResult
 - acc, 33
 - aux, 33
 - EvalResult, 31, 32
 - getAcc, 33
 - getAuxillery, 33
- at::iaik::mpc_acc::MPC_Acc
 - add, 40
 - CURVE1, 43
 - CURVE2, 44
 - close, 40
 - delete, 40
 - eval, 41
 - G1, 44
 - G2, 44
 - gen, 41
 - getRandomScalar, 41
 - getQ, 41
 - MPC_Acc, 40
 - mpc_params, 44
 - PAIRING, 44
 - pk2, 44
 - prepareBatches, 42
 - printAndResetComm, 42
 - Q, 44
 - random, 44
 - size, 44
 - sk_share, 45
 - verify, 42
 - witCreate, 43
 - witUpdate, 43
- at::iaik::mpc_acc::MPC_Add
 - acc, 46
 - buildComputation, 46
 - MPC_Add, 46
 - sk_share, 47
- at::iaik::mpc_acc::MPC_Del
 - acc, 49
 - buildComputation, 48
 - MPC_Del, 48
 - ro, 49
 - sk_share, 49
 - x, 49
- at::iaik::mpc_acc::MPC_Eval
 - buildComputation, 51
 - g1, 51
 - MPC_Eval, 50
 - sk_share, 51
 - X, 51
- at::iaik::mpc_acc::MPC_Gen
 - buildComputation, 53
 - g2, 53
 - MPC_Gen, 53
 - sk_share, 53
- at::iaik::mpc_acc::MPC_TripleDummy
 - LIMIT, 55
 - logger, 55
 - produceRandomFieldElements, 54
 - produceTriples, 55
- at::iaik::mpc_acc::MPC_WitCreate
 - acc, 57
 - buildComputation, 57
 - MPC_WitCreate, 57
 - ro, 57
 - sk_share, 58
 - x, 58
- at::iaik::mpc_acc::MPC_WitUpdateAdd
 - buildComputation, 59
 - MPC_WitUpdateAdd, 59
 - sk_share, 60
 - wit, 60
- at::iaik::mpc_acc::MPC_WitUpdateDel
 - buildComputation, 61
 - MPC_WitUpdateDel, 61
 - ro, 62
 - sk_share, 62
 - wit, 62
 - x, 62
- at::iaik::mpc_acc::MPCParams
 - closeNetwork, 71
 - getMyNetwork, 71
 - getMyNetworkManager, 71
 - getMyPool, 71
 - getMySce, 71
 - isLogging, 71
 - log, 71
 - shutdown, 71
 - shutdownSce, 71
- at::iaik::mpc_acc::MPCParamsBuilder
 - build, 73
 - MPCParamsBuilder, 73
- at::iaik::mpc_acc::Main
 - genList, 34
 - main, 34
 - SIZE, 35
- at::iaik::mpc_acc::MerkleTree
 - find, 37
 - getRootHash, 37
 - MerkleTree, 36
 - proof, 37
 - root, 38
 - round_up_to_power_of_2, 37
 - test, 38
 - verify, 38
- at::iaik::mpc_acc::MerkleTree::Position
 - left, 89
 - right, 89
- at::iaik::mpc_acc::MerkleTree::ProofNode
 - digest, 90
 - pos, 90
 - ProofNode, 90
- at::iaik::mpc_acc::Node
 - compute_digest, 84
 - digest, 84
 - left, 85

- Node, 83, 84
- right, 85
- at::iaik::mpc_acc::Polynomial
 - coeffs_, 88
 - degree_, 88
 - expand, 87
 - Polynomial, 87
 - powX, 88
 - toString, 88
- at::iaik::mpc_acc::Witness
 - element, 115
 - getElement, 114
 - getWitness, 114
 - Witness, 114
 - witness, 115
- at::iaik::utils::CmdLineParser
 - checkParty, 28
 - createPartyMap, 28
 - GetCmdLineParams, 29
 - IDERRMSG, 29
 - IDMSG, 29
 - LOGGINGMSG, 29
 - newID, 29
 - PARTYERRMSG, 30
 - PARTYMSG, 30
 - PRESTRATMSG, 30
 - SETERRMSG, 30
 - SETMSG, 30
- at::iaik::utils::CmdLineParser::BuilderParams
 - BuilderParams, 25
 - el, 26
 - evaluationStrategy, 26
 - id, 26
 - logging, 26
 - maxBitLength, 26
 - multiThreaded, 26
 - myParty, 26
 - parties, 26
 - partyList, 27
 - preprocessingStrategy, 27
 - setEl, 25
 - setEvaluationStrategy, 25
 - setId, 25
 - setMaxBitLength, 25
 - setParties, 25
 - setPreprocessingStrategy, 25
- at::iaik::utils::MPCBuilder
 - batchEvalStrat, 68
 - build, 64
 - computeSInts, 64
 - createPipe, 65
 - evaluate, 65
 - getDrbg, 66
 - getSeedOts, 66
 - log, 68
 - logging, 69
 - MPCBuilder, 64
 - maxBitLength, 69
 - myID, 69
 - myNetwork, 69
 - myNetworkConfiguration, 69
 - myNetworkManager, 69
 - myPool, 69
 - mySuite, 69
 - numberOfParties, 70
 - withBatchEvalStrat, 66
 - withID, 67
 - withNetwork, 67
 - withResourcePool, 67
 - withSpdzLength, 68
- at::iaik::utils::NetworkLoggingDecorator
 - close, 75
 - delegate, 76
 - getLoggedValues, 75
 - getNoOfParties, 76
 - NETWORK_PARTY_BYTES, 77
 - NETWORK_TOTAL_BATCHES, 77
 - NETWORK_TOTAL_BYTES, 77
 - NetworkLoggingDecorator, 75
 - partyStatsMap, 77
 - receive, 76
 - reset, 76
 - send, 76
- at::iaik::utils::NetworkLoggingDecorator::PartyStats
 - count, 86
 - noBytes, 86
 - recordTransmission, 85
- at::iaik::utils::NetworkManager
 - close, 79
 - configuration, 81
 - createExtraNetwork, 80
 - equalParties, 80
 - getLoggedValues, 80
 - getParties, 80
 - getPartyMap, 81
 - log, 81, 82
 - logging, 82
 - NetworkManager, 79
 - openedNetworks, 82
 - PORT_INCREMENT, 82
 - PORT_OFFSET_COUNTER, 82
 - partyMap, 82
 - portOffset, 82
 - reset, 81
 - UpdateConfiguration, 81
- aux
 - at::iaik::mpc_acc::EvalResult, 33
- Auxillery
 - at::iaik::mpc_acc::Auxillery, 21, 22
- Auxillery.java, 116
- batchEvalStrat
 - at::iaik::utils::MPCBuilder, 68
- build
 - at::iaik::mpc_acc::MPCParamsBuilder, 73
 - at::iaik::utils::MPCBuilder, 64
- buildComputation

- at::iaik::mpc_acc::MPC_Add, 46
- at::iaik::mpc_acc::MPC_Del, 48
- at::iaik::mpc_acc::MPC_Eval, 51
- at::iaik::mpc_acc::MPC_Gen, 53
- at::iaik::mpc_acc::MPC_WitCreate, 57
- at::iaik::mpc_acc::MPC_WitUpdateAdd, 59
- at::iaik::mpc_acc::MPC_WitUpdateDel, 61
- dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCMacCheckProtocol, 93
- BuilderParams
 - at::iaik::utils::CmdLineParser::BuilderParams, 25
- CURVE1
 - at::iaik::mpc_acc::Accumulator, 13
 - at::iaik::mpc_acc::AccumulatorDemo, 19
 - at::iaik::mpc_acc::MPC_Acc, 43
- CURVE2
 - at::iaik::mpc_acc::Accumulator, 13
 - at::iaik::mpc_acc::AccumulatorDemo, 19
 - at::iaik::mpc_acc::MPC_Acc, 44
- checkParty
 - at::iaik::utils::CmdLineParser, 28
- clearUpdate
 - at::iaik::mpc_acc::Auxillery, 22
- close
 - at::iaik::mpc_acc::MPC_Acc, 40
 - at::iaik::utils::NetworkLoggingDecorator, 75
 - at::iaik::utils::NetworkManager, 79
- closeNetwork
 - at::iaik::mpc_acc::MPCParams, 71
- closedValues
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCMacCheckProtocol, 94
- closedValuesECC
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCMacCheckProtocol, 94
- CmdLineParser.java, 116
- coeffs_
 - at::iaik::mpc_acc::Polynomial, 88
- compute_digest
 - at::iaik::mpc_acc::Node, 84
- computeSInts
 - at::iaik::utils::MPCBuilder, 64
- configuration
 - at::iaik::utils::NetworkManager, 81
- count
 - at::iaik::utils::NetworkLoggingDecorator::Party↔
Stats, 86
- createExtraNetwork
 - at::iaik::utils::NetworkManager, 80
- createPartyMap
 - at::iaik::utils::CmdLineParser, 28
- createPipe
 - at::iaik::utils::MPCBuilder, 65
- degree_
 - at::iaik::mpc_acc::Polynomial, 88
- delegate
 - at::iaik::utils::NetworkLoggingDecorator, 76
- Delete
 - at::iaik::mpc_acc::Accumulator, 10
 - at::iaik::mpc_acc::AccumulatorDemo, 16
- delete
 - at::iaik::mpc_acc::MPC_Acc, 40
- digest
 - at::iaik::mpc_acc::MerkleTree::ProofNode, 90
 - at::iaik::mpc_acc::Node, 84
- dk, 7
 - dk.alexandra, 7
 - dk.alexandra.fresco, 7
 - dk.alexandra.fresco.suite, 7
 - dk.alexandra.fresco.suite.spdz, 7
 - dk.alexandra.fresco.suite.spdz.ECCEExtension, 8
 - dk.alexandra.fresco.suite.spdz.ECCEExtension.SEC↔
Point, 91
 - dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzE↔
CCMacCheckProtocol, 92
 - dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzE↔
CCOps, 95
 - dk.alexandra.fresco.suite.spdz.ECCEExtension.SpdzE↔
CPoint, 99
 - dk.alexandra.fresco.suite.spdz.ECCEExtension.Spdz↔
KnownMultECCProtocol, 103
 - dk.alexandra.fresco.suite.spdz.ECCEExtension.Spdz↔
KnownScalar, 106
 - dk.alexandra.fresco.suite.spdz.ECCEExtension.Spdz↔
MultECCProtocol, 108
 - dk.alexandra.fresco.suite.spdz.ECCEExtension.Spdz↔
OpenedValueECCStoreImpl, 110
 - dk.alexandra.fresco.suite.spdz.ECCEExtension.Spdz↔
OutputPointProtocol, 111
 - dk::alexandra::fresco::suite::spdz::ECCEExtension::↔
SpdzECCMacCheckProtocol
 - alpha, 94
 - buildComputation, 93
 - closedValues, 94
 - closedValuesECC, 94
 - drbgByteLength, 94
 - jointDrbgSupplier, 95
 - modulus, 95
 - openedValues, 95
 - openedValuesECC, 95
 - sampleRandomCoefficients, 94
 - SpdzECCMacCheckProtocol, 93
 - dk::alexandra::fresco::suite::spdz::ECCEExtension::↔
SpdzECCOps
 - knownMultiply, 96
 - knownScalar, 97
 - multiply, 97
 - open, 97
 - protocolBuilder, 99
 - SpdzECCOps, 96
 - dk::alexandra::fresco::suite::spdz::ECCEExtension::↔
SpdzECPoint
 - getCurve, 101
 - getMac, 101
 - getShare, 101

- mac, [103](#)
- multiplyPoint, [102](#)
- out, [102](#)
- serialVersionUID, [103](#)
- serializeShare, [102](#)
- share, [103](#)
- SpdzECPPoint, [101](#)
- toString, [102](#)
- dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzKnownMultECCProtocol
 - evaluate, [105](#)
 - left, [105](#)
 - out, [105](#)
 - right, [105](#)
 - SpdzKnownMultECCProtocol, [104](#)
- dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzKnownScalar
 - evaluate, [107](#)
 - k, [107](#)
 - out, [107, 108](#)
 - SpdzKnownScalar, [107](#)
- dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzMultECCProtocol
 - evaluate, [109](#)
 - left, [110](#)
 - out, [109, 110](#)
 - right, [110](#)
 - SpdzMultECCProtocol, [109](#)
- dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzOutputPointProtocol
 - evaluate, [112](#)
 - in, [113](#)
 - out, [112, 113](#)
 - SpdzOutputPointProtocol, [112](#)
- drbgByteLength
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzECCMacCheckProtocol, [94](#)
- el
 - at::iaik::utils::CmdLineParser::BuilderParams, [26](#)
- element
 - at::iaik::mpc_acc::Witness, [115](#)
- equalParties
 - at::iaik::utils::NetworkManager, [80](#)
- Eval
 - at::iaik::mpc_acc::Accumulator, [10](#)
 - at::iaik::mpc_acc::AccumulatorDemo, [16](#)
- eval
 - at::iaik::mpc_acc::MPC_Acc, [41](#)
- EvalResult
 - at::iaik::mpc_acc::EvalResult, [31, 32](#)
- EvalResult.java, [116](#)
- evaluate
 - at::iaik::utils::MPCBuilder, [65](#)
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzKnownMultECCProtocol, [105](#)
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzKnownScalar, [107](#)
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzMultECCProtocol, [109](#)
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzOutputPointProtocol, [112](#)
- evaluationStrategy
 - at::iaik::utils::CmdLineParser::BuilderParams, [26](#)
- expand
 - at::iaik::mpc_acc::Polynomial, [87](#)
- find
 - at::iaik::mpc_acc::MerkleTree, [37](#)
- G1
 - at::iaik::mpc_acc::Accumulator, [13](#)
 - at::iaik::mpc_acc::AccumulatorDemo, [19](#)
 - at::iaik::mpc_acc::MPC_Acc, [44](#)
- g1
 - at::iaik::mpc_acc::MPC_Eval, [51](#)
- G2
 - at::iaik::mpc_acc::Accumulator, [13](#)
 - at::iaik::mpc_acc::AccumulatorDemo, [19](#)
 - at::iaik::mpc_acc::MPC_Acc, [44](#)
- g2
 - at::iaik::mpc_acc::MPC_Gen, [53](#)
- Gen
 - at::iaik::mpc_acc::Accumulator, [11](#)
 - at::iaik::mpc_acc::AccumulatorDemo, [17](#)
- gen
 - at::iaik::mpc_acc::MPC_Acc, [41](#)
- genList
 - at::iaik::mpc_acc::Main, [34](#)
- getAcc
 - at::iaik::mpc_acc::Auxillery, [22](#)
 - at::iaik::mpc_acc::EvalResult, [33](#)
- getAccPrime
 - at::iaik::mpc_acc::Auxillery, [22](#)
- getAuxillery
 - at::iaik::mpc_acc::EvalResult, [33](#)
- GetCmdLineParams
 - at::iaik::utils::CmdLineParser, [29](#)
- getCurve
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzECPPoint, [101](#)
- getDrbg
 - at::iaik::utils::MPCBuilder, [66](#)
- getElement
 - at::iaik::mpc_acc::Witness, [114](#)
- getList
 - at::iaik::mpc_acc::Auxillery, [22](#)
- getLoggedValues
 - at::iaik::utils::NetworkLoggingDecorator, [75](#)
 - at::iaik::utils::NetworkManager, [80](#)
- getMac
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
 - SpdzECPPoint, [101](#)
- getMyNetwork
 - at::iaik::mpc_acc::MPCParams, [71](#)
- getMyNetworkManager
 - at::iaik::mpc_acc::MPCParams, [71](#)

- getMyPool
 - at::iaik::mpc_acc::MPCParams, 71
- getMySce
 - at::iaik::mpc_acc::MPCParams, 71
- getNoOfParties
 - at::iaik::utils::NetworkLoggingDecorator, 76
- getParties
 - at::iaik::utils::NetworkManager, 80
- getPartyMap
 - at::iaik::utils::NetworkManager, 81
- getRandomScalar
 - at::iaik::mpc_acc::Accumulator, 11
 - at::iaik::mpc_acc::AccumulatorDemo, 17
 - at::iaik::mpc_acc::MPC_Acc, 41
- getRootHash
 - at::iaik::mpc_acc::MerkleTree, 37
- getSeedOts
 - at::iaik::utils::MPCBuilder, 66
- getShare
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECPoint, 101
- getUpdate
 - at::iaik::mpc_acc::Auxillery, 22
- getWitness
 - at::iaik::mpc_acc::Witness, 114
- getQ
 - at::iaik::mpc_acc::Accumulator, 11
 - at::iaik::mpc_acc::MPC_Acc, 41
- getR
 - at::iaik::mpc_acc::Auxillery, 22
- IDERRMSG
 - at::iaik::utils::CmdLineParser, 29
- IDMSG
 - at::iaik::utils::CmdLineParser, 29
- id
 - at::iaik::utils::CmdLineParser::BuilderParams, 26
- in
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzOutputPointProtocol, 113
- isLogging
 - at::iaik::mpc_acc::MPCParams, 71
- jointDrbgSupplier
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCMacCheckProtocol, 95
- k
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzKnownScalar, 107
- knownMultiply
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCOps, 96
- knownScalar
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCOps, 97
- LIMIT
 - at::iaik::mpc_acc::MPC_TripleDummy, 55
- LOGGINGMSG
 - at::iaik::utils::CmdLineParser, 29
- left
 - at::iaik::mpc_acc::MerkleTree::Position, 89
 - at::iaik::mpc_acc::Node, 85
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzKnownMultECCProtocol, 105
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzMultECCProtocol, 110
- list
 - at::iaik::mpc_acc::Auxillery, 23
- log
 - at::iaik::mpc_acc::MPCParams, 71
 - at::iaik::utils::MPCBuilder, 68
 - at::iaik::utils::NetworkManager, 81, 82
- logger
 - at::iaik::mpc_acc::MPC_TripleDummy, 55
- logging
 - at::iaik::utils::CmdLineParser::BuilderParams, 26
 - at::iaik::utils::MPCBuilder, 69
 - at::iaik::utils::NetworkManager, 82
- MPC_Acc
 - at::iaik::mpc_acc::MPC_Acc, 40
- MPC_Acc.java, 117
- MPC_Add
 - at::iaik::mpc_acc::MPC_Add, 46
- MPC_Add.java, 117
- MPC_Del
 - at::iaik::mpc_acc::MPC_Del, 48
- MPC_Del.java, 117
- MPC_Eval
 - at::iaik::mpc_acc::MPC_Eval, 50
- MPC_Eval.java, 117
- MPC_Gen
 - at::iaik::mpc_acc::MPC_Gen, 53
- MPC_Gen.java, 118
- MPC_TripleDummy.java, 118
- MPC_WitCreate
 - at::iaik::mpc_acc::MPC_WitCreate, 57
- MPC_WitCreate.java, 118
- MPC_WitUpdateAdd
 - at::iaik::mpc_acc::MPC_WitUpdateAdd, 59
- MPC_WitUpdateAdd.java, 118
- MPC_WitUpdateDel
 - at::iaik::mpc_acc::MPC_WitUpdateDel, 61
- MPC_WitUpdateDel.java, 119
- MPCBuilder
 - at::iaik::utils::MPCBuilder, 64
- MPCBuilder.java, 119
- MPCParams.java, 119
- MPCParamsBuilder
 - at::iaik::mpc_acc::MPCParamsBuilder, 73
- MPCParamsBuilder.java, 119
- mac
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECPoint, 103
- main
 - at::iaik::mpc_acc::Main, 34

- Main.java, 116
- maxBitLength
 - at::iaik::utils::CmdLineParser::BuilderParams, 26
 - at::iaik::utils::MPCBuilder, 69
- MerkleTree
 - at::iaik::mpc_acc::MerkleTree, 36
- MerkleTree.java, 117
- modulus
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCMacCheckProtocol, 95
- mpc_params
 - at::iaik::mpc_acc::MPC_Acc, 44
- multiThreaded
 - at::iaik::utils::CmdLineParser::BuilderParams, 26
- multiply
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCOps, 97
- multiplyPoint
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECPoint, 102
- myID
 - at::iaik::utils::MPCBuilder, 69
- myNetwork
 - at::iaik::utils::MPCBuilder, 69
- myNetworkConfiguration
 - at::iaik::utils::MPCBuilder, 69
- myNetworkManager
 - at::iaik::utils::MPCBuilder, 69
- myParty
 - at::iaik::utils::CmdLineParser::BuilderParams, 26
- myPool
 - at::iaik::utils::MPCBuilder, 69
- mySuite
 - at::iaik::utils::MPCBuilder, 69
- NETWORK_PARTY_BYTES
 - at::iaik::utils::NetworkLoggingDecorator, 77
- NETWORK_TOTAL_BATCHES
 - at::iaik::utils::NetworkLoggingDecorator, 77
- NETWORK_TOTAL_BYTES
 - at::iaik::utils::NetworkLoggingDecorator, 77
- NetworkLoggingDecorator
 - at::iaik::utils::NetworkLoggingDecorator, 75
- NetworkLoggingDecorator.java, 119
- NetworkManager
 - at::iaik::utils::NetworkManager, 79
- NetworkManager.java, 120
- newID
 - at::iaik::utils::CmdLineParser, 29
- noBytes
 - at::iaik::utils::NetworkLoggingDecorator::Party↔
Stats, 86
- Node
 - at::iaik::mpc_acc::Node, 83, 84
- Node.java, 120
- numberOfParties
 - at::iaik::utils::MPCBuilder, 70
- open
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCOps, 97
- openedNetworks
 - at::iaik::utils::NetworkManager, 82
- openedValues
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCMacCheckProtocol, 95
- openedValuesECC
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCMacCheckProtocol, 95
- out
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECPoint, 102
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzKnownMultECCProtocol, 105
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzKnownScalar, 107, 108
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzMultECCProtocol, 109, 110
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzOutputPointProtocol, 112, 113
- PAIRING
 - at::iaik::mpc_acc::Accumulator, 13
 - at::iaik::mpc_acc::AccumulatorDemo, 19
 - at::iaik::mpc_acc::MPC_Acc, 44
- PARTYERRMSG
 - at::iaik::utils::CmdLineParser, 30
- PARTYMSG
 - at::iaik::utils::CmdLineParser, 30
- PORT_INCREMENT
 - at::iaik::utils::NetworkManager, 82
- PORT_OFFSET_COUNTER
 - at::iaik::utils::NetworkManager, 82
- PRESTRATMSG
 - at::iaik::utils::CmdLineParser, 30
- parties
 - at::iaik::utils::CmdLineParser::BuilderParams, 26
- partyList
 - at::iaik::utils::CmdLineParser::BuilderParams, 27
- partyMap
 - at::iaik::utils::NetworkManager, 82
- partyStatsMap
 - at::iaik::utils::NetworkLoggingDecorator, 77
- pk
 - at::iaik::mpc_acc::Accumulator, 13
- pk2
 - at::iaik::mpc_acc::Accumulator, 13
 - at::iaik::mpc_acc::AccumulatorDemo, 19
 - at::iaik::mpc_acc::MPC_Acc, 44
- Polynomial
 - at::iaik::mpc_acc::Polynomial, 87
- Polynomial.java, 120
- portOffset
 - at::iaik::utils::NetworkManager, 82
- pos
 - at::iaik::mpc_acc::MerkleTree::ProofNode, 90
- powX
 - at::iaik::mpc_acc::Polynomial, 88

- prepareBatches
 - at::iaik::mpc_acc::MPC_Acc, 42
- preprocessingStrategy
 - at::iaik::utils::CmdLineParser::BuilderParams, 27
- printAndResetComm
 - at::iaik::mpc_acc::MPC_Acc, 42
- produceRandomFieldElements
 - at::iaik::mpc_acc::MPC_TripleDummy, 54
- produceTriples
 - at::iaik::mpc_acc::MPC_TripleDummy, 55
- proof
 - at::iaik::mpc_acc::MerkleTree, 37
- ProofNode
 - at::iaik::mpc_acc::MerkleTree::ProofNode, 90
- protocolBuilder
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCOps, 99
- Q
 - at::iaik::mpc_acc::Accumulator, 14
 - at::iaik::mpc_acc::AccumulatorDemo, 19
 - at::iaik::mpc_acc::MPC_Acc, 44
- r
 - at::iaik::mpc_acc::Auxillery, 23
- random
 - at::iaik::mpc_acc::Accumulator, 14
 - at::iaik::mpc_acc::AccumulatorDemo, 19
 - at::iaik::mpc_acc::MPC_Acc, 44
- receive
 - at::iaik::utils::NetworkLoggingDecorator, 76
- recordTransmission
 - at::iaik::utils::NetworkLoggingDecorator::Party↔
Stats, 85
- reset
 - at::iaik::utils::NetworkLoggingDecorator, 76
 - at::iaik::utils::NetworkManager, 81
- right
 - at::iaik::mpc_acc::MerkleTree::Position, 89
 - at::iaik::mpc_acc::Node, 85
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzKnownMultECCProtocol, 105
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzMultECCProtocol, 110
- ro
 - at::iaik::mpc_acc::MPC_Del, 49
 - at::iaik::mpc_acc::MPC_WitCreate, 57
 - at::iaik::mpc_acc::MPC_WitUpdateDel, 62
- root
 - at::iaik::mpc_acc::MerkleTree, 38
- round_up_to_power_of_2
 - at::iaik::mpc_acc::MerkleTree, 37
- SECPPoint.java, 120
- SETERRMSG
 - at::iaik::utils::CmdLineParser, 30
- SETMSG
 - at::iaik::utils::CmdLineParser, 30
- SIZE
 - at::iaik::mpc_acc::Main, 35
- sampleRandomCoefficients
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCMacCheckProtocol, 94
- send
 - at::iaik::utils::NetworkLoggingDecorator, 76
- serialVersionUID
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECPPoint, 103
- serializeShare
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECPPoint, 102
- setEI
 - at::iaik::utils::CmdLineParser::BuilderParams, 25
- setEvaluationStrategy
 - at::iaik::utils::CmdLineParser::BuilderParams, 25
- setId
 - at::iaik::utils::CmdLineParser::BuilderParams, 25
- setMaxBitLength
 - at::iaik::utils::CmdLineParser::BuilderParams, 25
- setParties
 - at::iaik::utils::CmdLineParser::BuilderParams, 25
- setPreprocessingStrategy
 - at::iaik::utils::CmdLineParser::BuilderParams, 25
- share
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECPPoint, 103
- shutdown
 - at::iaik::mpc_acc::MPCParams, 71
- shutdownSce
 - at::iaik::mpc_acc::MPCParams, 71
- size
 - at::iaik::mpc_acc::Accumulator, 14
 - at::iaik::mpc_acc::AccumulatorDemo, 20
 - at::iaik::mpc_acc::MPC_Acc, 44
- sk
 - at::iaik::mpc_acc::AccumulatorDemo, 20
- sk_share
 - at::iaik::mpc_acc::MPC_Acc, 45
 - at::iaik::mpc_acc::MPC_Add, 47
 - at::iaik::mpc_acc::MPC_Del, 49
 - at::iaik::mpc_acc::MPC_Eval, 51
 - at::iaik::mpc_acc::MPC_Gen, 53
 - at::iaik::mpc_acc::MPC_WitCreate, 58
 - at::iaik::mpc_acc::MPC_WitUpdateAdd, 60
 - at::iaik::mpc_acc::MPC_WitUpdateDel, 62
- SpdzECCMacCheckProtocol
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCMacCheckProtocol, 93
- SpdzECCMacCheckProtocol.java, 121
- SpdzECCOps
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECCOps, 96
- SpdzECCOps.java, 121
- SpdzECPPoint
 - dk::alexandra::fresco::suite::spdz::ECCEExtension↔
::SpdzECPPoint, 101
- SpdzECPPoint.java, 121

SpdzKnownMultECCProtocol
 dk::alexandra::fresco::suite::spdz::ECECExtension↔ at::iaik::utils::MPCBuilder, 67
 ::SpdzKnownMultECCProtocol, 104 withResourcePool
 at::iaik::utils::MPCBuilder, 67
 SpdzKnownMultECCProtocol.java, 121 withSpdzLength
 at::iaik::utils::MPCBuilder, 68
 SpdzKnownScalar
 dk::alexandra::fresco::suite::spdz::ECECExtension↔ Witness
 ::SpdzKnownScalar, 107 at::iaik::mpc_acc::Witness, 114
 SpdzKnownScalar.java, 121 witness
 at::iaik::mpc_acc::Witness, 115
 SpdzMultECCProtocol
 dk::alexandra::fresco::suite::spdz::ECECExtension↔ Witness.java, 122
 ::SpdzMultECCProtocol, 109
 SpdzMultECCProtocol.java, 122 X
 SpdzOpenedValueECCStoreImpl.java, 122 at::iaik::mpc_acc::MPC_Eval, 51
 SpdzOutputPointProtocol x
 dk::alexandra::fresco::suite::spdz::ECECExtension↔ at::iaik::mpc_acc::MPC_Del, 49
 ::SpdzOutputPointProtocol, 112 at::iaik::mpc_acc::MPC_WitCreate, 58
 SpdzOutputPointProtocol.java, 122 at::iaik::mpc_acc::MPC_WitUpdateDel, 62

t
 at::iaik::mpc_acc::Accumulator, 14

test
 at::iaik::mpc_acc::Accumulator, 11
 at::iaik::mpc_acc::AccumulatorDemo, 17
 at::iaik::mpc_acc::MerkleTree, 38

toString
 at::iaik::mpc_acc::Polynomial, 88
 dk::alexandra::fresco::suite::spdz::ECECExtension↔
 ::SpdzECPPoint, 102

update
 at::iaik::mpc_acc::Auxillery, 23

UpdateConfiguration
 at::iaik::utils::NetworkManager, 81

Verify
 at::iaik::mpc_acc::Accumulator, 12
 at::iaik::mpc_acc::AccumulatorDemo, 17

verify
 at::iaik::mpc_acc::MPC_Acc, 42
 at::iaik::mpc_acc::MerkleTree, 38

wit
 at::iaik::mpc_acc::MPC_WitUpdateAdd, 60
 at::iaik::mpc_acc::MPC_WitUpdateDel, 62

WitCreate
 at::iaik::mpc_acc::Accumulator, 12
 at::iaik::mpc_acc::AccumulatorDemo, 18

witCreate
 at::iaik::mpc_acc::MPC_Acc, 43

WitUpdate
 at::iaik::mpc_acc::Accumulator, 12
 at::iaik::mpc_acc::AccumulatorDemo, 18

witUpdate
 at::iaik::mpc_acc::MPC_Acc, 43

withBatchEvalStrat
 at::iaik::utils::MPCBuilder, 66

withID
 at::iaik::utils::MPCBuilder, 67

withNetwork