Input validation

Contact: Moryia

Go-ethereum changes:

- RequiredGas - Add check that the input has at least `FUNC_SIG_SIZE` bytes
- Adding input validation:
  - Ensures that the provided input contains at least `FUNC_SIG_SIZE+METADATA_SIZE` bytes to accommodate the function signature and metadata.
  - Checks that all provided parameters bit sizes adhere to the predefined set of supported bit sizes
  - Prevents mixing of boolean and integer parameters to avoid unintended behavior.
  - Ensures that requested parameters types are of supported types, preventing invalid or unrecognized data types from being processed.
  - Requires all parameters to be present and non-empty, avoiding potential null or undefined references.
  - Verifies that scalar inputs conform to the expected bit size.
  - Returns an error when input parameters size do not meet the required size constraints.
  - Converts the `shift` value from `int` to `uint` to prevent negative values and potential overflow scenarios.
  - Converts `offset` and `size` in `getEVMBytes` from `int` to `uint` to eliminate potential negative index errors and enhance memory safety.
  - Adjusts input length checks to enforce exact size requirements instead of using a general "less than" condition.
  - **Adds a verification step to ensure that the requested operation is valid for the given bit size, preventing unsupported computations.**

Soda-mpc changes:

Class::Function	Error	Change in Exception
Commons:: convertHexToBytes	Input hex string length is not even	runtime_error changed to invalid_argument

Commons:: convertHexToBytes	Output array does not have enough space for hex string	runtime_error changed to invalid_argument
Commons:: convertHexToBytes	Hex string parsing error	runtime_error changed to invalid_argument
Commons:: convertBitsToIntString	Cannot convert integer with more than 64 bits	runtime_error changed to invalid_argument
Commons:: generateRandomBoundedBits	Requested numBits is bigger than 64	runtime_error changed to invalid_argument
GarblingManager:: setCircuitsStatus	given circuits number is not equal to current circuits number	runtime_error changed to invalid_argument
OpcodesUtil:: convertStringToBcName	Invalid opcode name: <opcode_name>	runtime_error changed to invalid_argument
KMS:: getUserKey	Error while verifying the signature of the received data	runtime_error changed to invalid_argument
Secp256k1Utils:: ecrecover	Failed to parse compact signature	runtime_error changed to invalid_argument
Secp256k1Utils:: ecrecover	Failed to recover public key	runtime_error changed to invalid_argument
MPCEngine:: getOpOutputBitSize	Opname <op_name> not supported	runtime_error changed to invalid_argument

ProgramCompiler:: checkOpcode	Invalid input/output number	runtime_error changed to invalid_argument
ProgramCompiler:: checkOpcode	Opname <op_name> not supported	runtime_error changed to invalid_argument

Soda-mpc runtime_error cases (causing the chain to crash):

- Fail to compute basic operations:

Case	Message
Failed to open a file	`Failed to open the file <File_name>`
Failed to write to file	`Failed to write to file:<File_name>`
Failed to parse toml file	`Error parsing file <File_name>`

OpenSSL_ECDSA-
EVP_MD_CTX_new failed
EVP_DigestSignInit/EVP_DigestVerifyInit failed
EVP_DigestSign failed
	`Error creating MD context`
	`Error initializing digest sign`
	`Error creating signature`

OpenSSL_AESCTR -
EVP_CIPHER_CTX_new failed
EVP_DecryptInit_ex failed
EVP_EncryptUpdate failed
EVP_EncryptFinal_ex failed
	`Error creating cipher context`
	`Error initializing cipher context`
	`Error updating cipher context`
	`Error finalizing cipher context`

OpenSSL_hash - EVP_sha3_256/EVP_sha256/ EVP_MD_CTX_create failed EVP_DigestInit_ex failed	`Error: Failed to create hash context` `Error: Failed to initialize hash context`

OpenSSL_HMAC_SHA256- EVP_MAC_fetch EVP_MAC_CTX_new mac_ctx or mac are null EVP_MAC_init Hmac object is not initialized EVP_MAC_CTX_dup EVP_MAC_update EVP_MAC_final	Failed to fetch Hmac Failed to create MAC context MAC context or MAC not initialized Failed to initialize MAC context Hmac is not initialized Failed to clone MAC context Failed to update MAC Failed to finalize MAC
Garbler init files are missing/corrupted	Error while reading aes key AES key size is not correct Error while reading garbler key garbler key size is not correct
Evaluator init files are missing/corrupted	Error while reading evaluator key
Garbling manager has no garbling data for requested circuit	Error: Garbling data is nullptr
Failed to open evaluator batch data file	Could not open output file: <batch_data_file>
MongoDB is down	Error: Unable to connect to MongoDB server
GCManager startup - Batch is missing from the database	Missing batch id <batch_id> for circuit <circuit_name>
blState is negative	Invalid blState for circuit <circuit_name>
Gt's hash already exists in GTs map at the end of a circuit calculation	GT's hash already exists
Evaluator - failed to hash the gt	Failed to update the hash with the GT seed Failed to hash the output labels
Batch id is negative in batch file	Invalid batch ID: <batch_id>

KMS init files are missing/corrupted	`Error while reading aes key` `AES key size is not correct`
Secp256k1 library failed to create context	`Failed to create secp256k1 context`
No name specified in logger	`Name not set`
No role specified in stream communication	`Role is not initialized`
No private key provided to sign object	`Error: ECDSA cannot be used to sign, no signing key found`
Evaluator id is not 0/1	`Invalid party ID:<party_id>`

Soda-mpc - cases that would not happen in the current implementation:

Could not open input file - there is no input file in our case	`Could not open inputs file`

Old communication implementation	`Error creating client socket`
	`Failed to connect after timeout, aborting!`
	`Error creating server socket`
	`Error binding server socket on port <port>`
	`Error listening on server socket`
	`Error reading file <file_name>`

Failed to read ECDSA public key from file	`Unable to open public key file for reading` `Error reading public key from file`
Failed to read ECDSA private key from file	`Unable to open private key file for reading` `Error reading private key from file`
Failed to get address out of public key in openssl ECDSA - getSignerAdd function (no	`Error getting public key length` `Error getting public key`

one calls that function)	`Hash output is too small for an address`

OpenSSL RSAOAEP (used only in tests and simulator)	`Error creating RSA context`
	`Error initializing openssl keygen`
	`Error setting keygen parameters`
	`Error generating key`
	`Error setting RSA padding`
	`Error setting RSA OAEP hash function to SHA-256`
	`Error initializing openssl encrypt`
	`Error encrypting data`
	`Error: RSA cannot be used to decrypt, no private key found`
	`Error initializing openssl decrypt`
	`Error decrypting data`
	`Failed to create BIO`
	`Failed to write public key to BIO`
	`Failed to convert DER to EVP_PKEY`

Boolean circuit (unused)	`Invalid gate type`
	`Circuit file <file_name> not found`
	`Wrong number of inputs`
	`Wrong input`
	`Invalid truth table`

Benchmark mode	`Could not open benchmark file`