SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

秘密計算ライブラリ MEVAL3 における乗算の高速化実装について
A fast implementation of multiplication in the secure computation

橋本 順子 * 五十嵐 大 * 菊池 亮 *
Junko Hashimoto Dai Ikarashi Ryo Kikuchi

キーワード 秘密計算, 秘密分散, 秘密計算システム, 高速化

あらまし

秘密計算は平文に比べ複雑な処理や通信を行うため, 性能が課題となる. しかし秘密計算ライブラリ MEVAL3 [1] では, このようなハンデがあるにも関わらず, アルゴリズムの改善に加えて高速化実装を行うことで, 例えば秘密計算があまり得意でないソート処理においても平文比一桁差の性能を達成している.

本稿では, MEVAL3 における高速化実装について, 乗算を例に説明する. MEVAL3 では,(k, N)-Shamir 秘密分散方式を用いており，乗算アルゴリズムは Gennaro らの乗算 [2] を利用している．入力は $k = 2$, $N \geq 2k - 1$ を前提とし, 各サーバが持つ $(2, N)$-Shamir 秘密分散方式同士を乗算して $(3, N)$-Shamir 秘密分散方式の乗算結果のシェアを作成した後,$(2, N)$-Shamir 秘密分散方式で再分散し, 最終的に $(2, N)$-Shamir 秘密分散方式の乗算結果のシェアに変換する.

これを, サーバ, クライアント間でのシーケンスとして考えると, クライアントから N 台のサーバに乗算リクエストが発出された後,N 台のサーバ間で再分散のタイミングで通信を行い, 乗算結果をクライアントに返却する流れとなる.

従って, 高速化のポイントとしては, サーバ間の通信量の削減, サーバ間で通信を行う段数であるラウンド数の削減, 処理が滞留せず効率よく実行できる制御機構の実現, ローカル処理の高速化となる.

MEVAL3 は, 制御/プログラム解析部, プロトコル選択部, プロトコル定義部, プロトコル実行フレームワーク部, 代数演算部から構成される. これら各部の役割を高速化の観点から説明する.

- 制御/プログラム解析部: リクエスト受信後速やかに処理を開始するために,N 台のサーバ間でリクエストの内容・順番の一致を確認する. また, 不具合が発生した場合にキャンセル処理を行う.
- プロトコル選択部: 条件に一致した最適な (高速な) プロトコルを選択する.
- プロトコル定義部: 改ざん検知有無, 乱数生成方法, シェアの種類 ($Shamir/Additive$, サイズ）に応じた多数の秘密計算プロトコルを定義する.
- プロトコル実行フレームワーク部: 1 つのプロトコルをローカル処理単位のタスクに分解し, その粒度で並列処理を制御する. 制御系の通信を優先制御することで, 処理の効率化を図る.
- 代数演算部: タスク内での代数演算（主に秘密計算で用いる剰余体, 拡大体の演算）を行う. 代数演算レベル, 体に依存する高速化を行う.CPU 命令利用時のロジック, 通信用データ形式への変換など.

プロトコルの選択では, 改ざん検知有無, 乱数生成方法による通信量は, 最大のケースに対して $\frac{1}{8}$ となる. 通信用データ形式への変換では,61bit 剰余体を用いた場合, 通信量を 4.6% 削減する. このような技術の積み上げで MEVAL3 の高速化を実現している.

参考文献

[1] 桐淵直人, 五十嵐大, 濱田浩気, 菊池亮. プログラマブルな秘密計算ライブラリ MEVAL3. In *SCIS*, 2018.

[2] Rosario Gennaro, Michael O. Rabin, and Tal Rabin. Simplified VSS and fact-track multiparty computations with applications to threshold cryptography. In *PODC*, pp. 101–111, 1998.

* NTT 社会情報研究所, 東京都武蔵野市緑町 3-9-11, NTT Social Informatics Laboratories, 3-9-11. Midoricho, Musashino-shi, Tokyo, Japan junko.hashimoto.bx@hco.ntt.co.jp