Vol.2012-CSEC-58 No.40
Vol.2012-SPT-4 No.40
2012/7/20

計算量的秘密分散およびランプ型秘密分散のマルチパーティ計算拡張

千田 浩司[1]　五十嵐 大[1]　菊池 亮[1]　濱田 浩気[1]

概要：任意の線形秘密分散はマルチパーティ計算に拡張できることが知られているが，符号化効率の向上を目的とした計算量的秘密分散やランプ型秘密分散は一般にマルチパーティ計算への拡張が自明ではない．本稿では，SCIS2012 で筆者らが提案した，特定のマルチパーティ計算に拡張可能な計算量的秘密分散を再考し，単純な変形により計算量的秘密分散の分散情報を既存の各種マルチパーティ計算に適用できることを示す．また情報理論的安全性に基づくランプ型秘密分散について，準同型性を利用したマルチパーティ計算拡張手法を提案する．

キーワード：計算量的秘密分散，ランプ型秘密分散，線形秘密分散，マルチパーティ計算

Efficient Conversions from Computational SSS And Ramp SSS to Multi-Party Computation

Chida Koji[1]　Ikarashi Dai[1]　Kikuchi Ryo[1]　Hamada Koki[1]

Abstract: While Cramer et al. have provided a general multi-party computation protocol from any linear secret sharing scheme (linear SSS), it is NOT a trivial task in general how to develop *computational* SSSs and *ramp* SSSs into a multi-party computation. In this paper, we give a simple modification of the computational SSS, which we proposed at SCIS2012, so that some existing multi-party computation protocols can be achieved based on the modified computational SSS. We also develop *homomorphic* ramp SSSs with information-theoretic security into a general multi-party computation.

Keywords: Computational SSS, Ramp SSS, Linear SSS, Multiparty Computation

1. はじめに

重要データの耐消失性および機密性を両立させる技術として秘密分散が近年注目されている．例えば災害による重要データの消失を回避するため外部施設にバックアップデータを預けると，外部施設からの情報漏洩のリスクが新たに生じ，このような場合に秘密分散は有効とされる．

1979 年に Shamir[1] と Blakley[2] によって独立に提案された秘密分散は，$K \leq N$ を満たす 2 以上の整数 N, K について，元のデータを N 個に分散した分散情報を生成し，$N-K$ 個の分散情報が消失しても元のデータを復元できる耐消失性と，K 個未満の分散情報からは元のデータを一切復元できない機密性を合わせ持つ．

秘密分散の重要な課題として，符号化効率の向上が挙げられる．例えば Shamir が提案した秘密分散 [1](以降，Shamir 秘密分散と呼ぶ) は，個々の分散情報のサイズが元のデータのサイズと同程度になり，符号のサイズはおよそ N 倍になってしまう．符号化効率はストレージ容量や分散情報の送受信時間に影響するため，**計算量的秘密分散** [3] や**ランプ型秘密分散** [4], [5] といった符号化効率の向上を目的とした秘密分散が研究されている．

一方，元のデータを復元することなく，分散情報から算術演算や検索といったデータ処理ができる**マルチパーティ計算**が提案されている [6], [7], [8]．マルチパーティ計算は一般に，各計算主体 $\mathrm{P}_i (i = 1, \ldots, N)$ がそれぞれ値 a_i を

[1] NTT セキュアプラットフォーム研究所

持つとき，他の主体に a_i を明かすことなく，所定の関数値 $f(a_1,\ldots,a_N)$ を得る技術の総称である．例えば a_i をある値 a の分散情報とし，$f(a_1,\ldots,a_N)$ を a の算術演算や検索の結果と見ることができる．

[6], [7] では Shamir 秘密分散のマルチパーティ計算拡張手法を与えている．また [8] では，後述する任意の**線形秘密分散**をマルチパーティ計算に拡張できることを示している．しかし符号化効率の向上を目的とした計算量的秘密分散やランプ型秘密分散に対するマルチパーティ計算拡張の研究は，筆者らが知る限りほとんどない．

筆者らは SCIS2012 において，先ず [3] の方式と同程度の符号化効率を持つ計算量的秘密分散を提案し，次にその分散情報から「Shamir 秘密分散のマルチパーティ計算拡張に適用可能な分散情報」を求める**分散情報変換**手法を提案した [9]．これにより，符号化効率が良い計算量的秘密分散のマルチパーティ計算拡張を可能にした．

本稿では，[9] の単純な変形により，分散情報変換を用いて計算量的秘密分散の分散情報を既存の各種マルチパーティ計算に適用できることを示す．また，準同型性を持つ任意のランプ型秘密分散のマルチパーティ計算拡張手法を提案する．

2. 関連研究

分散情報の数を N とし，元のデータの復元に必要な分散情報の最小十分数（閾値）が K となる秘密分散は，(K,N) 閾値秘密分散と呼ばれる．Shamir 秘密分散は，K 未満の分散情報からは無条件に元のデータを復元できない，すなわち情報理論的安全性を持つ (K,N) 閾値秘密分散である．情報理論的安全性を持つ (K,N) 閾値秘密分散は，分散情報のサイズの下限が元のデータのサイズとなり符号化効率が悪い．

情報理論的安全性を持つ秘密分散において，元のデータを復元できる分散情報の集合は有資格集合と呼ばれ，全く情報が得られない分散情報の集合は禁止集合と呼ばれる [10]．これに対してランプ型秘密分散は，有資格集合でも禁止集合でもない中間的な分散情報の集合を許すことで符号化効率を向上させている．分散情報の数を N とし，閾値が K，そして中間的な分散情報の集合の最小要素数が $K-L+1$ となる秘密分散は，(K,L,N) 閾値ランプ型秘密分散と呼ばれる．(K,L,N) 閾値ランプ型秘密分散における分散情報のサイズの下限は，元のデータのサイズの $1/L$ となる．なお L はその取り方から $L<K$ の関係を満たす必要がある．

計算量的秘密分散は，計算量的安全性を持つ秘密分散であり，符号化効率の向上を目的とする．Krawczyk は，元のデータを共通鍵暗号で暗号化し，共通鍵は所定の (K,N) 閾値秘密分散を用いて分散するが，暗号文は符号化効率が良い IDA (Information Dispersal Algorithm)[*1] [11] を用いて分散する，(K,N) 閾値計算量的秘密分散を提案した [3]．共通鍵の符号のサイズは元のデータのサイズよりも十分小さいと仮定して無視すれば，(K,N) 閾値計算量的秘密分散の分散情報のサイズの下限は，元のデータのサイズの $1/K$ となる．

Cramer らは任意の線形秘密分散をマルチパーティ計算に拡張できることを示した [8]．ここで線形秘密分散とは，F を有限体として，元のデータ $a\in F$ について全ての分散情報は $a\in F$ および F 上の乱数の線形結合で表現できる秘密分散と定義される．例えば，Shamir 秘密分散は線形秘密分散だが，[3] の計算量的秘密分散は線形秘密分散ではなく，マルチパーティ計算への拡張が自明ではない．

植松と岩村は，Shamir 秘密分散を変形し，$K-1$ 個までの分散情報のサイズを小さくできる (K,N) 閾値計算量的秘密分散を提案した [12]．彼らが提案した計算量的秘密分散は線形秘密分散ではないが，後述するようにマルチパーティ計算への拡張は容易である．

筆者らは [9] において，[12] の方式の変形として，分散情報のサイズがほぼ下限となる (K,N) 閾値計算量的秘密分散を提案した．また，[6], [7] 等の Shamir 秘密分散のマルチパーティ計算拡張に適用可能な分散情報を求める分散情報変換手法を提案した．ただし [9] の分散情報変換は Shamir 秘密分散のマルチパーティ計算拡張に限定される．したがって，処理速度向上のため環 $\mathbb{Z}_{2^{32}}$ 上の演算を採用しているマルチパーティ計算 [13] 等への拡張はできない．

2.1 Shamir 秘密分散

元のデータを有限体 $F=GF(p)$ の元 $a\in F$ として，$f_a(0)=a$ となる $K-1$ 次式 $f_a(x)$ から分散情報 $f_a(i)$ $(i=1,\ldots,N)$ を求める．すると $1\le n_1,\ldots,n_K\le N$ について，K 個の互いに異なる分散情報 $f_a(n_1),\ldots,f_a(n_K)$ から，以下の Lagrange 補間式により $a=f_a(0)$ を復元できる．

$$f_a(x)=\sum_{i=1}^{K} f_a(n_i)L_i(x) \qquad (1)$$

$$L_i(x)=\prod_{j=1,j\neq i}^{K}\frac{x-n_j}{n_i-n_j}$$

Shamir 秘密分散は線形秘密分散であり，**（加法）準同型性**を持つ．すなわち $a,b\in F$ の分散情報 $f_a(i),f_b(i)$ および $a+b$ の分散情報 $f_{a+b}(i)$ について，$f_a(i)+f_b(i)=f_{a+b}(i)$ が成り立つ．

符号化効率：$|f_a(i)|=|a|$（$=|F|$）より，個々の分散情報のサイズは元のデータのサイズと等しく，符号のサイズは $N|F|$ となる（任意の x について，$|x|$ は x のサイズを表す）．

[*1] IDA 自体は一般に元データの機密性を保証しない．

2.2 ランプ型秘密分散

[14] の方式に基づく，Shamir 秘密分散を変形した (K, L, N) 閾値ランプ型秘密分散を例示する．

元のデータを有限体 $F = GF(p)$ の元の L 次ベクトル $a = (a_1, \ldots, a_L) \in F^L$ として，$f_a(N+j) = a_j$ $(j = 1, \ldots, L)$ となる $K-1$ 次式 $f_a(x)$ から分散情報 $f_a(i)$ $(i = 1, \ldots, N)$ を求める．すると $1 \le n_1, \ldots, n_K \le N$ について，K 個の互いに異なる分散情報 $f_a(n_1), \ldots, f_a(n_K)$ から，式 (1) より $a_j = f_a(N+j)$ を復元できる．

上記のランプ型秘密分散は，$a, b \in F^L$ の分散情報 $f_a(i), f_b(i)$ および $a+b$ の分散情報 $f_{a+b}(i)$ について，$a + b = (a_1 + b_1, \ldots, a_L + b_L)$ とすれば $f_a(i) + f_b(i) = f_{a+b}(i)$ が成り立つため加法準同型性を持つ．しかし [8] ではランプ型秘密分散については言及されておらず，マルチパーティ計算拡張の実現可能性は明らかでない．

符号化効率：$|f_a(i)| = |a|/L$ より，分散情報のサイズは元のデータのサイズの $1/L$ となり，符号のサイズは $N|F|/L$ となる．

2.3 計算量的秘密分散

ここでは 3 つの計算量的秘密分散方式を紹介する．後述するように，何れも準同型性を持たず線形秘密分散ではないが，植松と岩村の方式 [12]，および筆者らの従来方式 [9] はマルチパーティ計算に拡張可能である．

2.3.1 Krawczyk の方式 [3]

[3] の方式に基づく，Shamir 秘密分散を変形した (K, N) 閾値計算量的秘密分散を例示する．

元のデータを有限体 $F = GF(p)$ の元の K 次ベクトル $a = (a_1, \ldots, a_K) \in F^K$ として，$E : \mathcal{K} \times F^K \to F^K$ を鍵 $k \in \mathcal{K}$ および元のデータ $a \in F^K$ から暗号文 $c = (c_1, \ldots, c_K) \in F^K$ を求める暗号化関数とする．このとき，k を $\mathcal{K}$ からランダムに選び暗号文 $c = E(k, a)$ を計算し，Shamir 秘密分散を用いて k の分散情報 $f_k(i)$ $(i = 1, \ldots, N)$ を求め，IDA を用いて $g_c(N+j) = c_j$ $(j = 1, \ldots, K)$ となる $K-1$ 次多項式 $g_c(x)$ から c の分散情報 $g_c(i)$ $(i = 1, \ldots, N)$ を求め，a の分散情報 $(f_k(i), g_c(i))$ $(i = 1, \ldots, N)$ を得る．復元の手順は 2.2 節の説明から明らかなため省略する．

上記の計算量的秘密分散は，暗号化関数の適用により，一般に準同型性を持たず線形秘密分散とはならない．

符号化効率：鍵 k の符号のサイズは $|F|$ と比べて十分小さいと仮定して無視すれば，$|f_k(i)| + |g_c(i)| \approx |g_c(i)| = |a|/K$ より，分散情報のサイズは元のデータのサイズの $1/K$ となり，符号のサイズは $N|F|/K$ となる．これらは (K, N) 閾値秘密分散の下限である．

2.3.2 植松と岩村の方式 [12]

Shamir 秘密分散同様，元のデータを有限体 $F = GF(p)$ の元 $a \in F$ として，$f_a(0) = a$ となる $K-1$ 次式 $f_a(x)$ から分散情報 $f_a(i)$ $(i = 1, \ldots, N)$ を求める．ただし $K-1$ 個のシード $s_1, \ldots, s_{K-1} \in \mathcal{S}$ および疑似乱数生成関数 $P : \mathcal{S} \to F$ を用いて，$f_a(i) = P(s_i)$ $(i = 1, \ldots, K-1)$ とする．そして分散情報 $f_a(1), \ldots, f_a(K-1)$ をそれぞれ $s_1, \ldots, s_{K-1}$ に置き換え，復元時に限り $f_a(i) = P(s_i)$ を計算して $a = f_a(0)$ を復元する．

一般に P は線形関数でないため，上記の計算量的秘密分散は準同型性を持たず線形秘密分散とはならない．しかし $P(s_1), \ldots, P(s_{K-1}), f_a(K), \ldots, f_a(N)$ を a の分散情報として [6], [7] 等のマルチパーティ計算拡張に適用できる[*2]．

符号化効率：$|\mathcal{S}|$ は $|F|$ と比べて十分小さいと仮定して $|s_i|$ を無視すれば，符号のサイズは $(N-K+1)|F|$ となる．

2.3.3 筆者らの従来方式 [9]

分散情報の生成は既存方式の単純な組み合わせであり，[12] の方式の分散情報 $s_1, \ldots, s_{K-1}$ および $f_a(K)$ について，$s_1, \ldots, s_{K-1}$ の各々を Shamir 秘密分散を用いて分散し，$f_a(K)$ を [3] の (K, N) 閾値計算量的秘密分散を用いて分散する[*3]．なお $f_a(K+1), \ldots, f_a(N)$ の生成は不要となる．すると $s_1, \ldots, s_{K-1}$ および $f_a(K)$ はそれぞれ K 個の分散情報から復元でき，$f_a(i) = P(s_i)$ $(i = 1, \ldots, K-1)$ を求めれば，式 (1) より $a = f_a(0)$ を復元できる．

マルチパーティ計算拡張は，計算主体 P_i $(i = 1, \ldots, K)$ が $f_a(i)$ を復元し，他の主体に $f_a(i)$ を明かすことなく，計算主体 P_j $(j = K+1, \ldots, N)$ のみが新たに $f_a(j)$ を得る分散情報変換からなり，例えば [15] の方式を用いて実現できる．

符号化効率：シード $s_1, \ldots, s_{K-1}$ の符号のサイズは $|F|$ と比べて十分小さいと仮定して無視すれば，分散情報のサイズおよび符号のサイズは IDA と等しくなり，分散情報のサイズは元のデータのサイズのおよそ $1/K$，そして符号のサイズは $N|F|/K$ となる．

3. 提案方式

(1) [9] の一般化．具体的には，(K, N) 閾値計算量的秘密分散の分散情報を既存の各種マルチパーティ計算に適用できることを示す．

(2) [8] で言及されていない情報理論的安全性に基づくランプ型秘密分散について，準同型性を持つ (K, L, N) 閾値ランプ型秘密分散であれば，既存の各種マルチパーティ計算に拡張できることを示す．

3.1 [9] の一般化

[16] の方式に基づき [9] の方式を単純に変形することで，以下に示すように (K, N) 閾値計算量的秘密分散の分散情

[*2] ただし $P(s_i)$ は疑似乱数のため，[6], [7] 等のマルチパーティ計算拡張に適用した場合は情報理論的安全性を持たない．

[*3] [9] では，[3] の (K, N) 閾値計算量的秘密分散ではなく IDA としているが，IDA では機密性を保証できない．

報を既存の各種マルチパーティ計算に適用できる．

3.1.1 分散

(1) 環 R 上の元のデータ $a \in R$ を入力する．
(2) $K-1$ 個のシード $s_1, \ldots, s_{K-1} \in \mathcal{S}$ および疑似乱数生成関数 $P : \mathcal{S} \to R$ を用いて $f_a(i) = P(s_i)$ $(i = 1, \ldots, K-1)$ を計算する．
(3) $f_a(K) = a - \sum_{i=1}^{K-1} f_a(i)$ を計算する．
(4) R 上の任意の (K, N) 閾値秘密分散を用いて $s_1, \ldots, s_{K-1}$ および $f_a(K)$ を分散し，これらの分散情報の組を a の分散情報とする．

符号化効率：上記のステップ（4）で用いる (K, N) 閾値秘密分散に依存するが，[3] の方式を用いて $f_a(K)$ を分散すれば，分散情報のサイズおよび符号のサイズは [3] の方式と同等になる．

3.1.2 復元

(1) a の K 個の異なる分散情報から $s_1, \ldots, s_{K-1}$ および $f_a(K)$ を復元する．
(2) $f_a(i) = P(s_i)$（$i = 1, \ldots, K-1$）を計算する．
(3) $a = \sum_{i=1}^{K} f_a(i)$ を復元する．

3.1.3 分散情報変換

(1) 計算主体 P_i（$i = 1, \ldots, K$）は $S_i = f_a(i)$ を入力し，準同型性を持つ R 上の任意の (K, N) 閾値秘密分散を用いて S_i を分散し，分散情報 $f_{S_i}(j)$（$j = 1, \ldots, N$）を計算主体 P_j に送信する．
(2) 計算主体 P_j（$j = 1, \ldots, N$）はステップ（1）で用いた (K, N) 閾値秘密分散の準同型性を利用して $a = \sum_{i=1}^{K} S_i$ の分散情報 $g_a(j) = \sum_{i=1}^{K} f_{S_i}(j)$ を得る．

3.1.4 効果

3.1.3 節の分散情報変換で生成した a の分散情報 $g_a(j)$ は，環 R 上の任意の (K, N) 閾値秘密分散の分散情報とできるため，環 $\mathbb{Z}_{2^{32}}$ 上で演算を行うマルチパーティ計算 [13] を含め既存の各種マルチパーティ計算拡張に適用できる．

3.1.5 機密性

3.1.1 節の分散において各計算主体が得る情報は，R 上の任意の (K, N) 閾値秘密分散を用いた K 個の分散情報であり，各分散情報に互いに独立な乱数を用いれば，利用した (K, N) 閾値秘密分散の機密性に帰着される．

3.1.3 節の分散情報変換において全ての計算主体が得る情報は，準同型性を持つ R 上の任意の (K, N) 閾値秘密分散を用いた K 個の分散情報であり，これは分散時同様に各分散情報に互いに独立な乱数を用いれば，利用した (K, N) 閾値秘密分散の機密性に帰着される．さらに計算主体 P_i $(i = 1, \ldots, K)$ は $a = \sum_{i=1}^{K} S_i \in R$ を満たす S_i を得るが，これは前述の K 個の分散情報と独立にでき，各計算主体が持つ K 個全ての S_i を得ない限り a の情報は得られないため，結局，利用した (K, N) 閾値秘密分散の機密性に帰着される．

3.2 ランプ型秘密分散のマルチパーティ計算拡張

準同型性を持つ環 R 上の任意の (K, L, N) 閾値ランプ型秘密分散は既存の各種マルチパーティ計算に拡張できることを示す．基本的なアプローチは，元のデータ $a = (a_1, \ldots, a_L) \in R^L$ の分散情報 $f_a(i)$ について，準同型性を利用して乱数 $r = (r_1, \ldots, r_L) \in R^L$ を加えた分散情報 $f_{a+r}(i)$ を求めて $c = a + r$，すなわち $c_j = a_j + r_j$ $(j = 1, \ldots, L)$ を復元し，次に準同型性を持つ R 上の任意の (K, N) 閾値秘密分散を用いて c_j（$j = 1, \ldots, L$）を分散し，分散情報 $f_{c_j}(i)$ から準同型性を利用して乱数 r_i を取り除き，a_j の分散情報 $f_{a_j}(i) = f_{c_j - r_j}(i)$ を得る．

3.2.1 分散情報変換

(1) 計算主体 P_i（$i = 1, \ldots, K$）は以下を行う．
  (a) 準同型性を持つ環 R 上の任意の (K, L, N) 閾値ランプ型秘密分散を用いた元のデータ $a = (a_1, \ldots, a_L) \in R^L$ の分散情報 $f_a(i)$ を入力する．
  (b) L 個の乱数 $r_{i,1}, \ldots, r_{i,L} \in R$ を生成し，前記の (K, L, N) 閾値ランプ型秘密分散を用いて $r_i = (r_{i,1}, \ldots, r_{i,L})$ を分散し，分散情報 $f_{r_i}(j)$ $(j = 1, \ldots, N)$ を計算主体 P_j に送信する．
  (c) 準同型性を持つ環 R 上の任意の (K, N) 閾値秘密分散を用いて $r_{i,1}, \ldots, r_{i,L} \in R^L$ を分散し，分散情報 $g_{r_{i,h}}(j)$ $(h = 1, \ldots, L,\ j = 1, \ldots, N)$ を計算主体 P_j に送信する．
  (d) 前記の (K, L, N) 閾値ランプ型秘密分散の準同型性を利用して $a + \sum_{i=1}^{K} r_i$ の分散情報 $f_{a+\sum_{i=1}^{K} r_i}(j)$ $(j = 1, \ldots, N)$ を求めて計算主体 P_1 に送信する．
(2) P_1 は以下を行う．
  (a) $a + \sum_{i=1}^{K} r_i$（すなわち $a_h + \sum_{i=1}^{K} r_{i,h}$ $(h = 1, \ldots, L)$）を復元する．
  (b) 前記の (K, N) 閾値秘密分散を用いて $c_h = a_h + \sum_{i=1}^{K} r_{i,h}$（$h = 1, \ldots, L$）を分散し，分散情報 $g_{c_h}(j)$（$j = 1, \ldots, N$）を計算主体 P_j に送信する．
(3) 計算主体 P_j（$j = 1 \ldots, N$）は前記の (K, N) 閾値秘密分散の準同型性を利用して $a_h = c_h - \sum_{i=1}^{K} r_{i,h}$ の分散情報 $g_{a_h}(j) = g_{c_h}(j) - \sum_{i=1}^{K} g_{r_{i,h}}(j)$ を得る．

3.2.2 効果

情報理論的安全性を持つ符号化効率が良い (K, L, N) 閾値ランプ型秘密分散について，準同型性を持てばマルチパーティ計算に拡張できる．また 3.1.4 節と同様に，3.2.1 節で与えた，a_h（$h = 1, \ldots, L$）の分散情報 $g_{a_h}(j)$ は，環 R 上の任意の (K, N) 閾値秘密分散の分散情報とできるため，既存の各種マルチパーティ計算に適用できる．

3.2.3 機密性

3.2.1 節の分散情報変換プロトコルにおいて全ての計算主体が得る情報は，準同型性を持つ R 上の任意の (K, L, N) 閾値ランプ型秘密分散および (K, N) 閾値秘密分散を用い

た分散情報であり，これは各分散情報に互いに独立な乱数を用いれば，利用した (K, L, N) 閾値ランプ型秘密分散および (K, N) 閾値秘密分散の機密性に帰着される．さらに計算主体 P_i （$i = 1, \ldots, K$）は $a = (a_1, \ldots, a_L)$ の分散情報 $f_a(i)$ を得るが，これは前述の分散情報と独立にでき，利用した (K, L, N) 閾値ランプ型秘密分散の機密性に帰着される．

最後に計算主体 P_1 だけが得る情報については，各計算主体が生成した乱数の和が加えられているため a の情報は得られない．

4. まとめ

本稿では，符号化効率が良い計算量的秘密分散をマルチパーティ計算に拡張した筆者らの先行研究について，単純な変形により既存の各種マルチパーティ計算への拡張が可能なことを示した．また同様に，情報理論的安全性を持つ符号化効率が良い閾値ランプ型秘密分散においても，準同型性を持てば，既存の各種マルチパーティ計算への拡張が可能なことを具体例により示した．

謝辞 文献 [12] についてご紹介して頂いた，東京理科大学の岩村惠市教授に感謝いたします．

参考文献

[1] Shamir, A.: How to share a secret. Commun. ACM 22(11), pp. 612–613 (1979)
[2] Blakley, G. R.: Safeguarding cryptographic keys. Proc. of the National Computer Conference 48, pp. 313–317 (1979)
[3] Krawczyk, H.: Secret sharing made short. CRYPTO 1993, pp.136–146 (1993)
[4] 山本: (k, L, n) しきい値秘密分散システム. 電子通信学会論文誌, vol.J68-A, no.9, pp. 46–54 (1986)
[5] Blakley, G.R. and Meadows, C.: Security of ramp schemes. CRYPTO 1984, pp. 242–269 (1985)
[6] Ben-Or, M., Goldwasser, S., and Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). STOC 1988, pp. 1–10 (1988)
[7] Chaum, D., Crépeau, C., and Damgård, I.: Multiparty unconditionally secure protocols (extended abstract) STOC 1988, pp. 11–19 (1988)
[8] Cramer, R., Damgård, I., and Maurer, U.: General secure multi-party computation from any linear secret-sharing scheme. Eurocrypto 2000, pp. 316–334 (2000)
[9] 千田, 五十嵐, 濱田, 菊池, 冨士, 高橋: マルチパーティ計算に適用可能な計算量的ショート秘密分散. SCIS 2012 (2012)
[10] 山本: 秘密分散法とそのバリエーション. 数理解析研究所講究録, 1361 巻, pp. 19–31 (2004)
[11] Rabin, M. O.: Efficient dispersal of information for security, load balancing, and fault tolerance. J. ACM 36(2), pp.335–348 (1989)
[12] 植松, 岩村: 複数の情報を有するメモリやデータベースに適した秘密分散法. SCIS 2011 (2011)
[13] Bogdanov, D., Laur, S., and Willemson, J.: Sharemind: a framework for fast privacy-preserving computations. ESORICS 2008, pp. 192–206 (2008)
[14] 滝澤: 多項式補間法による強いランプ型しきい値秘密分散法. 信州大学学士論文 (2009)
[15] Herzberg, A., Jarecki, S., Krawczyk, H., and Yung, M.: Proactive secret sharing Or: How to cope with perpetual leakage. CRYPTO 1995, pp. 339–352 (1995)
[16] Laur, S., Willemson, J., and Zhang, B.: Round-efficient oblivious database manipulation. ISC 2011, pp. 262–277 (2011)