Vol.2013-CSEC-62 No.16
Vol.2013-SPT-6 No.16
2013/7/18

巡回置換行列を用いず m 次元数ベクトル空間を用いて XOR 演算だけで構成可能な $(2, 2^m)$-閾値秘密分散法

須賀 祐治[1,a)]

概要：排他的論理和演算を用いた高速な (k, n)-閾値秘密分散法は栗原ら，藤井らによって独立に提案されている．彼らの方式はともにシェアのサイズが分散対象データのサイズに等しい理想的な方式であり，分散・復元時に XOR 演算のみを用いるため非常に高速に処理できるメリットを持つ．一方で素数位数の巡回置換行列を用いて構成しているため，シェア数 n は素数であるという制限があった．ここで分散対象データは $n-1$ 個に等分割されている．
この制約に対し CSS2012 にて素数 p に対し，分散対象データを $p-1$ 個に等分割して $(2, p+1)$-閾値秘密分散法を一般的に構成する方法が提案された．本稿はさらにこれを拡張し，任意の 2 以上の整数 m に対して分散対象データを m 個に等分割して $(2, 2^m)$-閾値秘密分散法の構成方法について提案する．提案方式の構成にはある条件を満たした基底を持つ $\mathbb{Z}_2$ 上の m-次元数ベクトル空間が用いられる．ここで，構成に用いられる基底集合として 2-伝播基底集合という新しい概念を定義する．さらに $(2, 2^m)$-閾値秘密分散法の存在性を保証するために，2-伝播基底集合の存在性についても触れる．

キーワード：閾値秘密分散法, 排他的論理和演算, 理想的な秘密分散法, $\mathbb{Z}_2^m$ 上の基底

An exclusive-OR operations based $(2, 2^m)$-threshold secret sharing scheme using m-dimensional vector spaces over $\mathbb{Z}_2$ instead of circulant permutation matrices

Yuji Suga[1,a)]

Abstract: Fast (k, n)-threshold secret sharing schemes with exclusive-OR operations have proposed by Kurihara et al. and Fujii et al. independently. Their method are ideal that share size is equal to the size of the data to be distributed with the benefits that can be handled very fast for using only XOR operation at distribution and restoration processes. In these cases for the number of shares n, target data must be equally divided into individual $n_p - 1$ pieces where n_p is a prime more than n.
The existing methods described above are configured using the cyclic matrices with prime order. On the other hand, a new method in CSS2012 have proposed, this leads to general constructions of $(2, p+1)$-threshold secret sharing schemes.
In this paper, we use m-dimensional vector spaces over $\mathbb{Z}_2$ on having bases that meet certain conditions in order to construct proposed methods. This paper defines a new notion "2-propagation bases set" as a bases set to be used in the configuration. In order to guarantee the existence of $(2, 2^m)$-threshold secret sharing schemes, we also treat the presence of the m-dimensional bases.

Keywords: (k, n)-threshold secret sharing scheme, exclusive-OR operation, ideal secret sharing scheme, bases over $\mathbb{Z}_2^m$

Vol.2013-CSEC-62 No.16
Vol.2013-SPT-6 No.16
2013/7/18

1. はじめに

本稿は排他的論理和を用いた $(2, 2^m)$-閾値秘密分散法の新しい構成とその優位性について述べる．本方式はクラウドコンピューティングにおける利用に適していることを示すために，まずクラウドにおけるセキュリティ上の課題について整理する．

1.1 クラウドにおけるセキュリティ要件

近年，クラウドの構成・標準化について検討するためのコミュニティが乱立しており，各々がそれぞれのスタンスでクラウドとか何かについて定義している [1], [2], [3], [4], [5]. 本稿では Open Cloud Manifesto[6] によるクラウドの特徴「必要に応じた処理能力を低コストで確保でき，その能力を手軽に利用できる」を紹介するに留める．またクラウドの用途として，パブリッククラウドとプライベートクラウドに分類することが多い．パブリッククラウドはインターネットなどオープンに提供されているクラウドを指す．一方プライベートクラウドは企業等の閉じたネットワークで利用されるなど，全ての権限をコントロール配下に置く専用クラウドと捉えることができる．パブリッククラウドとプライベートクラウドは用途，特に扱われる情報の重要度に応じて使い分けがなされている．

一般的なセキュリティ要件の考え方を論じる際に用いる CIA(Confidentiality, Integrity and Availability) モデルを用いてクラウド**ならでは** のセキュリティ要件について分類が検討されている [7]．実際にはこの 3 要件だけではなく，クラウドでは境界の問題を筆頭に様々な観点でのセキュリティ分析が必要である．本稿ではこれ以上の議論を取り扱わないが文献 [8] を参考文献として挙げておく．

以下 CIA それぞれの要件に呼応する対策の動向について整理する．

完全性

ID 連携技術の適用領域としてクラウド間連携（インタークラウド）が，グローバルクラウド基盤連携技術フォーラム（GICTF）[9] や OASIS Identity In the Clouds TC[10] で議論されつつある．カンターライニシアティブの技術をそのまま利用できるメリットを生かし SAML, OpenID など 異なる仕様間での連携をクラウド間で行うメリットはあるが，クラウドならではの要件については小さいと考えられる．

可用性

SLA(Service Level Agreement) による利用者にサービスの品質を保証する制度の SaaS 版として経済産業省が取りまとめたガイドライン [13] には，サービス稼働率，平均復旧時間，データ消去の要件，通信の暗号化レベルに関する取り決めの例が掲載されている．

また「クラウド事業者の信頼性」に対するお墨付き制度として SAS 70 type II[11] や FMMC による「ASP・SaaS 安全・信頼性情報開示認定制度」[12] などが存在する．

秘匿性

クラウドにおける秘匿性要件は，上記の 2 つの要件とは異なり多くの検討が行われている．これは，個人向けクラウド（個人情報：電子メール，画像，住所録，家計簿），企業向けクラウド（社内機密情報，顧客情報），官公庁向けクラウド（国家機密情報，住民情報）において「商用のクラウドサービス業者に安心してデータを預けられるか？」という疑問が明瞭であることに起因すると考えられる．

この不安に対する解決策として次の技術について列挙しておく．分散データを秘密にしたままデータマイニングする Privacy-preserving Data Mining [14], 検索キーを秘匿したまま（暗号化された）検索結果を取得する Searchable Encryption [15] のほか，暗号化データを（信頼していない）クラウドに計算作業を委託して計算結果を入手可能にする Gentry による Fully Homomorphic Encryption [16] はその後改良 [17] が続けられている．また岡本-高島方式 [18] は復号条件が AND，OR，NOT 演算，閾値ゲートにより構成される関係式で表現可能であり，より柔軟性の高い復号形態を持つためクラウド環境に適した暗号方式として注目されている．このように実用的なツールとして近づきつつある．

1.2 After 3.11 のニーズ移行

東日本大震災以降，ディザスタリカバリや事業継続計画に対する関心が高まっている．具体的には安定的な電力供給が見込めない，もしくは地震の余波によるネットワーク遮断の可能性からクラウドリソースを利用できない状況が鑑みられている．またデータセンターへの物理的な被害により，データ紛失という問題も考えられる．この可用性の課題に対して秘密分散共有法のクラウド適用の検討が試みられている．

秘密分散共有法

秘密分散共有法 (Secret Sharing Scheme; SSS) は，前述した CIA モデルによれば秘匿性と可用性の要件をバランスよく持つ技術として認識されており文献 [19] などにより提案された概念である．例えば最もシンプルな例の一つとして (k, n)-しきい値秘密分散法が存在する．秘密情報 S を n 個の分散情報（シェア）に符号化し配布した状態で，任意の k 個の分散情報からは S を復号可能であるが，任意の $k-1$ 個の分散情報からは S に関する情報は全く得られないという性質を持つ．本技術の導入効果として１）漏洩リスクの分散（一部漏洩しても暴露されない），２）紛失

[1] 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc., Jinbocho Mitsui Bldg. 1-105 Kandajinbo-cho, Chiyoda-ku, Tokyo, 101-0051, Japan
[a)] suga@iij.ad.jp

リスクの分散（一部紛失しても復元可能）の 2 つがあり，アプリケーション，ユースケースに応じて上記パラメータ n, k を選択できる自由度を持つ．

秘密分散技術適用におけるビジネス上の課題

実際に秘密分散共有技術をクラウド環境でサービスイン [20], [21] する動きも見受けられる．しかし公開情報からはサービスを構成するための具体的な技術要素が不明瞭である．そのため，クラウドサービス事業者が不正する，構成方法自体が脆弱であるなどの事由により，顧客から預かった情報が復元できてしまう可能性がある．このビジネス上の課題に対して，何がしかの技術適用とその技術の確からしさを顧客に提示することが必要である．しかし「なんとなく」安心&安全に使えるクラウドサービスではあってはならない．顧客への説明責任を踏まえ，シェアの一部を利用者側でプライベートクラウドとして運用するというビジネスモデルを好む顧客も潜在的には存在するとも考えられる．可用性要件の節で前述したように「お墨付き制度」だけでクラウド事業者を選択するのではなく，透明性のあるセキュリティ技術を提供することで，顧客への安心感を提供するべきである．

そこで本稿では，クラウド事業者が顧客からのデータをアーカイブし，顧客の要求に応じてデータを処理するケース，特に利用頻度の低いバックアップなどのデータアーカイブとしての用途において，クラウドでの利用に適した秘密分散共有法の利用方法を提案する．

1.3 本稿の構成

2 章にてデータフローモデルを整理し，既存の排他的論理和演算で構成される秘密分散法 (XOR-SSS) がクラウドでの利用に適していることを示す．3 章にて XOR-SSS そのものに対する新しい提案方式を示し，さらにランプ型秘密分散への適用も行う．最後に 4 章にてまとめと今後の課題について紹介する．

2. データフローモデル

データをアーカイブする際にクラウド事業者は，前章で述べたように秘匿性と可用性を高めるために，1）データ暗号化，2）秘密分散共有法の両方を併用すると考えられる．また，クラウド事業者は不測のデータクラッシュなどの障害に対処するため，やはり可用性を高めるために，顧客から預かったデータを主体の異なる他の事業者にコピーもしくはデータの一部を暗号化・秘密分散処理を行った上で再配布を行うというケースを考える．

2.1 データフローの分類

1）データ暗号化と 2）秘密分散共有法の両方を併用する場合には，図 1 に示すように E 型と F 型の 2 つのフローが考えられる．E 型は 1）データ暗号化→2）秘密分散共有法の処理順（左回り），F 型はその逆で 2）秘密分散共有法→1）データ暗号化の処理順（右回り）と考えればよい．

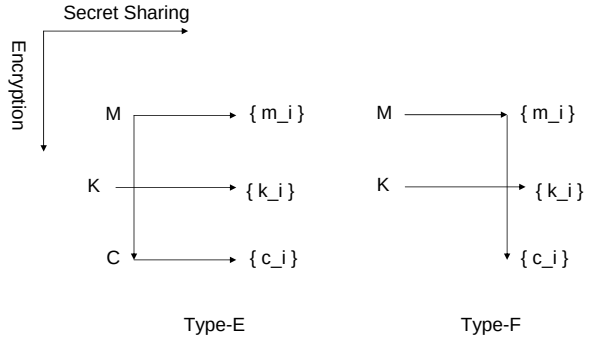

図 1 データフローモデル

暗号化処理においては，顧客データ M を鍵 K で暗号化したデータを C と表記する．また秘密分散処理においては，データ D をシェア（分散データ）d_i に分散すると表記する．E 型，F 型ともに，暗号処理に用いた鍵を秘密分散して委託するケースも考えられる点に留意する．この場合，鍵だけではなく，暗号化データとともに格納するケースでは，格納するクラウド事業者をそれぞれ異なる主体に委託するなどの考慮が必要となる．

2.2 データ処理要件

前述のデータフローモデルにおいては，以下のことに留意する必要がある．アーカイブ依頼されたクラウド事業者は，異なる主体の事業者にデータを複製する場合，意図せず同一主体が qualified sets のひとつを得てしまうケースを避ける必要がある．復元権限を得たクラウド事業者は不正またはサーバ等をクラックされることにより，顧客データを復元できてしまうためである．

これを避けるためには，顧客からどのようにデータが伝播しているかについて知ることができるように配慮すべきである．これは，事業者間のデータフローだけでなく，同一事業者内においてデータを複製・分散しているケースでも同様である．このとき上記のデータフロー図などの表記法を用いて視覚化し，常時顧客に伝えることができると考えられる．

2.3 本稿が解決すべき課題

複数のクラウドで複製，分散が繰り返されている顧客データの断片を復元・復号するフェーズを考える．その際には前述したデータフロー図を遡ることで復元・復号作業を行うことが一般的であると考えられる．しかしこのサービスは必ずしも対称である必要はない．つまり図 2 にように，リクエストに対するレスポンスを当該リスクエストサービスが返答する必要はない．例えば，ネットワークトポロジーを鑑み，最も転送に効率のよい経路を選択する，

課金が最も低いクラウドサービスから優先的に選択する，など，クラウドサービスの連携により，より良い選択肢をユーザに与えるビジネスモデルの提供が望まれる．

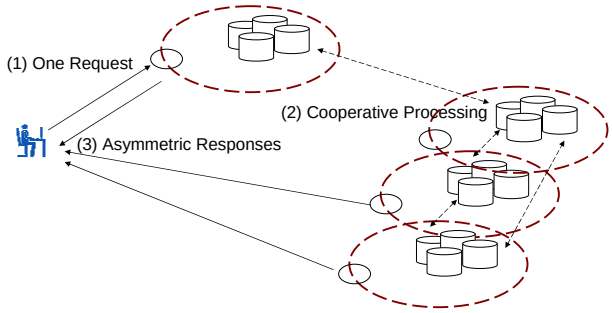

図 2 非対称なクラウドサービス

この連携サービスにおいては，各クラウド共通の標準的な API，フォーマットなどの準備が必要であるが，処理レベルに鑑みると図 3 のように新しい要件として「秘密分散処理とデータ暗号化の可換性」が必要であることがわかる．本稿では，準同型性を有する関数を用いることで実現可能かどうかを検討したが，処理速度を考慮し，排他的論理和 (XOR) 演算の可換性を用いた方法について検討を行った．

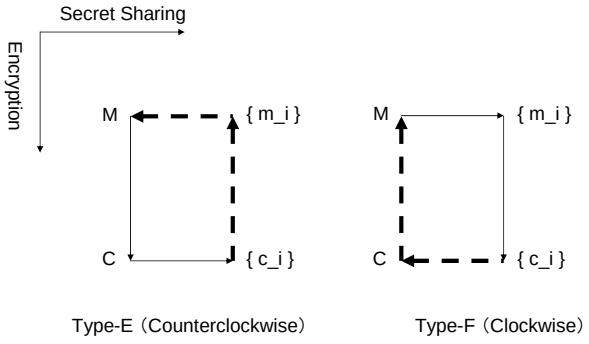

図 3 E 型,F 型における復元処理サイクル

具体的には，複数の暗号化・分散処理を経て，数ホップ先に格納されたデータ群から，復元に必要なデータに直接アクセスして転送・復元処理を行うことで，処理速度を軽減する技術が有益である．このとき，本モデルはクラウドサービスの信頼度から，クラウドサービスにデータ復元委託を行うケースも含まれていることに留意する．

2.4 暗号化と秘密分散の両立

本章にて排他的論理和演算の可換性という特徴を用い従来の秘密分散法に適用可能な復元・復号方式について説明する．前章の図 3 のように分散/復元サイクルを構成するためには，暗号化処理としてストリーム暗号やブロック暗号での CTR モード利用など，平文にキーストリームを XOR で足し込む演算を用いる．また秘密分散処理として，排他的論理和演算で構成される秘密分散法を用いることで，暗号（復号）処理と秘密分散（復元）処理の順序を変更することが可能となり，分散/復元サイクルが実現できる．

排他的論理和演算で構成される秘密分散法

排他的論理和演算で構成される (k,n)-しきい値秘密分散方式 (XOR-(k,n)-SSS) は藤井, 多田ら [22], [23], [24]，栗原ら [25], [26] によって独立に提案されている．シンプルな具体例として [22] に記載の XOR-$(2,3)$-SSS について説明する．秘密情報 $M = M_1||M_2$（M_i のサイズは d ビット）に対して d ビットデータ R_0, R_1 を生成し，シェア $W_i (i = 0, 1, 2)$ を

W_0	$(M_0 \oplus R_0) \,\|\|\, (M_2 \oplus R_1)$
W_1	$(M_1 \oplus R_0) \,\|\|\, (M_0 \oplus R_1)$
W_2	$(M_2 \oplus R_0) \,\|\|\, (M_1 \oplus R_1)$

とおくことで構成可能である．ただし $||$ はデータの連結を，$\oplus$ はビットごとの排他的論理和を示し M_0 は各ビットが全て 0 で構成されているものとする．本方式は，各シェアサイズが分散対象のデータサイズと同じとなる理想的な秘密分散法式となっている．

データ暗号化と秘密分散処理が可換な方式

ここで M_i として暗号化データを代入，つまりキーストリーム K_i との XOR 演算結果 $K_i \oplus M_i$ を代入する（ストリーム暗号やブロック暗号にて CTR モードを利用する）ことにより，暗号化処理と秘密分散処理が可換であることは自明である．例えば E 型（暗号化→秘密分散）の場合，前述の XOR-$(2,3)$-SSS においては，暗号処理 $M_i \to K_i \oplus M_i$ を施したあと秘密分散処理を行う，つまり，

W_0	$((K_0 \oplus M_0) \oplus R_0) \,\|\|\, ((K_2 \oplus M_2) \oplus R_1)$
W_1	$((K_1 \oplus M_1) \oplus R_0) \,\|\|\, ((K_0 \oplus M_0) \oplus R_1)$
W_2	$((K_2 \oplus M_2) \oplus R_0) \,\|\|\, ((K_1 \oplus M_1) \oplus R_1)$

とシェアを構成すればよい．ここで，暗号化と秘密分散処理を行う主体が同一である場合には K_0 を各ビットが 0 の NULL データとしても一般性を失わない．E 型復元（復号→秘密復元）処理においては XOR 演算が可換であることから $((K_i \oplus M_i) \oplus R_i) \oplus K_i = M_i \oplus R_i$ が成立することにより，本方式が正しく動作することがわかる．

また，F 型（秘密分散処理→暗号化）の場合，

W_0	$(M_0 \oplus R_0) \oplus K'_{0L} \,\|\|\, (M_2 \oplus R_1) \oplus K'_{0R}$
W_1	$(M_1 \oplus R_0) \oplus K'_{1L} \,\|\|\, (M_0 \oplus R_1) \oplus K'_{1R}$
W_2	$(M_2 \oplus R_0) \oplus K'_{2L} \,\|\|\, (M_1 \oplus R_1) \oplus K'_{2R}$

とシェアを構成し，F 型復元（秘密復元→復号）処理においては $(M_i \oplus K'_{**}) \oplus K'_{**} = M_i$ がが成立することにより，E 型復元と同様に本方式が正しく動作することがわかる．

暗号化処理と復号処理の主体が同一かどうかによって鍵データ K'_{**} をどのように配備するか復元処理を顧客側も

しくはトラストなクラウドサービスで行うケースにおいては M_i に関わる K'_{**} を同じように構成することで秘密復元と復号を同時に行うことができるメリットを有する．

上記は XOR-$(2,3)$-SSS のみについて具体的に扱ったが，任意の XOR-(k,n)-SSS [24], [26] においても，分散・復元フェーズにおいて XOR 演算のみを用いているため容易に拡張可能であることは自明である．

3. XOR-$(2,n)$-SSS 構成方法の再考

本章では $k=2$ を満たす XOR 演算だけを用いた秘密分散方式の構成方法を考察していく．ターゲットデータ M の分割数を $n^{'}$ とすると XOR-$(2,n)$-SSS のシェア $W_i(i=0,\ldots,n)$ を次のマトリクスで表現することとする．ここで $n^{''} := n^{'}-1$，$W_i = W_{i0} \,||\, \ldots \,||\, W_{in''}$ とする．

W_0	W_{00}	$\ldots$	$W_{0n''}$
W_1	W_{10}	$\ldots$	$W_{1n''}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$
W_i	W_{i0}	$\ldots$	$W_{in''}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$
W_n	W_{n0}	$\ldots$	$W_{nn''}$

3.1 栗原らの方式 [26]

まず巡回置換行列を用いた XOR-$(2,n)$-SSS の構成方式について説明する．素数 n_p に対して $n=n_p$ となる XOR-$(2,n)$-SSS with $n^{'}=n_p-1$ をシェア $W_i(i=0,\ldots,n_p-1)$ は $n^{'}$ 個 $W_{ij}(j=0,\ldots,n^{'}-1)$ のパーツ の連結と考える．ターゲットデータ M は $M_1,\ldots,M_{n'}$ の連結で各データ長を d ビット，$M_0 \in \{0\}^d$ とする．また M_0 と同じサイズのダミーデータ $R_i(i=0,\ldots,n_p)$ をランダムに選択する．このとき W_{ij} を $M_j \oplus R_{(j-i) \mod n_p}$ とおく．

上記構成方式に基づいて構成される XOR-$(2,3)$-SSS with $n^{'}=2$ は以下の通りである．

Example1 (XOR-$(2,3)$-SSS [26]) $M = M_1 || M_2$ $(n^{'}=2), M_0 \in \{0\}^d$

W_0	$M_0 \oplus R_0$	$M_1 \oplus R_1$
W_1	$M_2 \oplus R_0$	$M_0 \oplus R_1$
W_2	$M_1 \oplus R_0$	$M_2 \oplus R_1$

さらに $n_p=5$ のときに構成される XOR-$(2,5)$-SSS with $n^{'}=4$ は以下の通りである．

Example2 (XOR-$(2,5)$-SSS [26])

W_0	$M_0 \oplus R_0$	$M_1 \oplus R_1$	$M_2 \oplus R_2$	$M_3 \oplus R_3$
W_1	$M_4 \oplus R_0$	$M_0 \oplus R_1$	$M_1 \oplus R_2$	$M_2 \oplus R_3$
W_2	$M_3 \oplus R_0$	$M_4 \oplus R_1$	$M_0 \oplus R_2$	$M_1 \oplus R_3$
W_3	$M_2 \oplus R_0$	$M_3 \oplus R_1$	$M_4 \oplus R_2$	$M_0 \oplus R_3$
W_4	$M_1 \oplus R_0$	$M_2 \oplus R_1$	$M_3 \oplus R_2$	$M_4 \oplus R_3$

3.2 CSS2012 方式 [27]

栗原らの方式 [26] では素数 n_p に対して $n^{'}=n_p-1=n-1$ でしか構成できないという制約があった．これを解消するために以下のように CSS2012 方式 [27] が提案されている．

素数 n_p に対して $n=n_p+1$ となる XOR-$(2,n)$-SSS with $n^{'}=n_p-1$ をシェア $W_i(i=0,\ldots,n_p)$ は $n^{'}$ 個 $W_{ij}(j=0,\ldots,n^{'}-1)$ のパーツ の連結と考える．ターゲットデータ M は $M_1,\ldots,M_{n'}$ の連結で各データ長を d ビット，$M_0 \in \{0\}^d$ とする．また M_0 と同じサイズのダミーデータ $R_i(i=0,\ldots,n_p)$ をランダムに選択する．このとき W_{ij} を以下のようにおく．

- $W_{00}=R_0$
- $W_{0j}=M_1 \oplus M_{j+1} \oplus R_j \quad (j=1,\ldots,n^{'}-1)$
- $W_{10}=M_1 \oplus R_0$
- $W_{1j}=W_{0,j-1} \oplus R_{j-1} \oplus R_j$ $(j=1,\ldots,n^{'}-1)$
- $W_{ij}=W_{i-1,j-1} \oplus R_{j-1} \oplus R_j$ $(i=2,\ldots,n^{'}-1, j=1,\ldots,n^{'}-1)$
- $W_{n',j}=M_2 \ \oplus,\ldots,\oplus \ M_{n'} \oplus R_j$ $(j=1,\ldots,n^{'}-1)$

上記構成方式に基づいて構成される XOR-$(2,4)$-SSS with $n^{'}=2 \neq n-1=3$ は以下の通りである．

Example3 (XOR-$(2,4)$-SSS [27]) $M = M_1 || M_2$ $(n^{'}=2), M_0 \in \{0\}^d$

W_0	$M_0 \oplus R_0$	$M_1 \oplus M_2 \oplus R_1$
W_1	$M_1 \oplus M_2 \oplus R_0$	$M_1 \oplus R_1$
W_2	$M_1 \oplus R_0$	$M_0 \oplus R_1$
W_3	$M_2 \oplus R_0$	$M_2 \oplus R_1$

$F()$ を複数のシェアを入力すると，各パートで復元されるデータを出力する関数と考える．例えば $F(\{W_0,W_1\}) = \{M_1 \oplus M_2$ (左パート) $, M_2$ (右パート) $\}$ となり結果的に M_1, M_2 の両方を復元することが可能となる．以下他のケースについても

- $F(\{W_0,W_2\}) = \{M_1, M_1 \oplus M_2\}$,
- $F(\{W_0,W_3\}) = \{M_2, M_1\}$,
- $F(\{W_1,W_2\}) = \{M_2, M_1\}$,
- $F(\{W_1,W_3\}) = \{M_1, M_1 \oplus M_2\}$,
- $F(\{W_2,W_3\}) = \{M_1 \oplus M_2, M_2\}$.

となり M_1, M_2 の両方を復元することがわかる．

さらに $n_p=5$ のときに構成される XOR-$(2,6)$-SSS with $n^{'}=4$ は以下の通りである．ただし $M_{234} := M_2 \oplus M_3 \oplus M_4$ とおく．

Example4 (XOR-$(2,6)$-SSS [27])

W_0	$M_0 \oplus R_0$	$M_1 \oplus M_2 \oplus R_1$	$M_1 \oplus M_3 \oplus R_2$	$M_1 \oplus M_4 \oplus R_3$
W_1	$M_1 \oplus R_0$	$M_0 \oplus R_1$	$M_1 \oplus M_2 \oplus R_2$	$M_1 \oplus M_3 \oplus R_3$
W_2	$M_1 \oplus M_4 \oplus R_0$	$M_1 \oplus R_1$	$M_0 \oplus R_2$	$M_1 \oplus M_2 \oplus R_3$
W_3	$M_1 \oplus M_3 \oplus R_0$	$M_1 \oplus M_4 \oplus R_1$	$M_1 \oplus R_2$	$M_0 \oplus R_3$
W_4	$M_1 \oplus M_2 \oplus R_0$	$M_1 \oplus M_3 \oplus R_1$	$M_1 \oplus M_4 \oplus R_2$	$M_1 \oplus R_3$
W_5	$M_{234} \oplus R_0$	$M_{234} \oplus R_1$	$M_{234} \oplus R_2$	$M_{234} \oplus R_3$

3.3 XOR-$(2,n)$-SSS における同型性の導入

上記例のようにシェアを表現するマトリクス $\{W_{ij}\}$ に対して，次のように同型性を定義する．

Definition5 (XOR-$(2,n)$-SSS における同型性) XOR-$(2,n)$-SSS Ψ の W_{ij} 成分がマトリクス表現されているとき，以下の操作に基づいて変形されたマトリクスから生成される XOR-$(2,n)$-SSS は Ψ と同型であるとする．

(1) ある行を他の行と入れ替える
(2) ある列を他の列と入れ替える
(3) ある列の全てのサブシェアのそれぞれに対して同じデータを XOR で足し込む

(1) については配布されるシェアの index が変更したのみであり (2) についてはシェアの各パートの順番が変更されたに過ぎず配布されるデータとしては同一である．(3) については足し込むランダムデータ R_i に変化が生じたに過ぎず，選択されたランダムデータが異なるだけであると解釈できる．つまり，上記操作を行ったとしても安全性を確保しつつ，別の異なる XOR-$(2,n)$-SSS を構成することが可能である．ただしシェア生成時の効率性については増減する場合があることは自明である．

次に Example1 をもとに実際の変形例を見ることにする．

Example6 (Example1 の変形例)

W_0	$M_0 \oplus R_0$	$M_0 \oplus R_1^{'}$
W_1	$M_2 \oplus R_0$	$M_1 \oplus R_1^{'}$
W_2	$M_1 \oplus R_0$	$M_1 \oplus M_2 \oplus R_1^{'}$

上記例はサブシェア $W_{t1}(t=0,\ldots,2)$ に M_1 を足しこんだデータと同一である．ランダムデータとして R_1 ではなく $R_1^{'}$ と記載しているがランダムデータの選択には依存しないため以降は R_i と記載しても問題ない．次に Example3 を変形して Example1 との拡張性を見い出す．下記例は Example3 においてサブシェア $W_{t1}(t=0,\ldots,2)$ に $M_1 \oplus M_2$ を足しこんだデータである．

Example7 (Example3 の変形例)

W_0	$M_0 \oplus R_0$	$M_0 \oplus R_1$
W_1	$M_1 \oplus M_2 \oplus R_0$	$M_2 \oplus R_1$
W_2	$M_1 \oplus R_0$	$M_1 \oplus M_2 \oplus R_1$
W_3	$M_2 \oplus R_0$	$M_1 \oplus R_1$

これを Example6 と比較すると Example7 では W_1 が新たに追加された拡張方式であることがわかる．

XOR-SSS をシェアを表現する方式として上記例のマトリクス表現ではなく，各サブシェア W_{ij} を次のように $\mathbb{Z}_2^{n^{'}}$ の元として表現することとする．$W_{ij} = \bigoplus_{t=1}^{n^{'}} \alpha_t M_t$ のとき $w_{ij} = (\alpha_1,\ldots,\alpha_{n'}) \in \mathbb{Z}_2^{n^{'}}$ とベクトル表現を行う．このとき各列に同じように出現するランダムデータのパート R_i およびゼロデータ M_0 は無視しても一般性を失わない．

以下例は Example6 をベクトル表現に変換したものである．

Example8 (Example7 のベクトル表現)

W_0	$(0,0)$	$(0,0)$
W_1	$(1,1)$	$(0,1)$
W_2	$(1,0)$	$(1,1)$
W_3	$(0,1)$	$(1,0)$

4. 2-伝播基底集合の定義と XOR-$(2,2^m)$-SSS への展開

前章で取り上げた XOR-$(2,4)$-SSS のトイケースを Example8 のようにベクトル表現したとき，各列のベクトルが $n^{'}$ 次元ベクトル空間を構成していることが分かる．具体的には Example8 において $w_{10} = w_{20} + w_{30}, w_{11} = w_{21} + w_{31}$ を満たしている．ここで + は $\mathbb{Z}_2^m$ 上の加算を意味する．

この例に見られるように m 次ベクトル空間から XOR-$(2,2^m)$-SSS を構成する可能性について本章にて議論していく．その準備のためはじめにいくつかの定義を行う．

$\mathbb{Z}_2^m$ を張る基底 $b = b^{(1)}, b^{(2)}, \ldots, b^{(m)}$ を考える．ここで $b^{(i)}$ は m 次元ベクトルである．このとき $\mathbb{Z}_2^m$ の元は $\sum_{i=1}^{m} \alpha_i b^{(i)}$ for $\alpha_i \in \mathbb{Z}_2$ と表現できる．

Definition9 (基底の和) 2 つの基底 b_i, b_j に対して基底の和を次のように定義する．$b_i + b_j := \{b_i^{(1)} + b_j^{(1)}, b_i^{(2)} + b_j^{(2)}, \ldots, b_i^{(m)} + b_j^{(m)}\}$．ここで + は $\mathbb{Z}_2^m$ 上の加算を意味する．

Remark10 (XOR 演算と $\mathbb{Z}_2^m$ 上の加算の関係) 2 つの m 次元ベクトル $b^{(i)}, b^{(j)} \in \mathbb{Z}_2^m$ の $\mathbb{Z}_2^m$ 上の加算はビットごとの排他的論理和と同一視できる．例：$(0,0,1,1) + (0,1,0,1) = (0,1,1,0) \in \mathbb{Z}_2^4$.

4.1 2-伝播基底集合の定義とその性質

Definition11 (2-伝播基底集合) $\mathbb{Z}_2^m$ を張る基底 $\{b_i\}(i=1,\ldots,l)$ の集合が以下の条件を満たすとき $\{b_i\}$ を 2-伝播基底集合という： b_1 は全てゼロベクトルで構成される（便宜上 b_1 も基底と同一視する）．任意の異なる 2 つの基底 b_i, b_j に対して $b_i + b_j$ が $\mathbb{Z}_2^m$ の基底となる．

Definition12 (k-伝播基底) 3 以上の k に対して 2-伝播基底と同様に以下のように k-伝播基底を定義することが可能である．$\mathbb{Z}_2^m$ を張る基底 $\{b_i\}$ の集合が k-伝播基底であるとは，任意の異なる k 個の基底 $b_{i_1},\ldots,b_{i_k}$ に対して $\sum_{j=i_1,\ldots,i_k} b_j$ が $\mathbb{Z}_2^m$ の基底となることと定義する．本稿では利用しないがこの概念を用いることで XOR-$(k,2^m)$-SSS もしくはランプ型 XOR-$(k,2^m)$-SSS を構成することができると考えられる．

Theorem13 (2-伝播基底集合の位数) $\mathbb{Z}_2^m$ 上の 2-伝播基底集合 $\{b_i\}$ の位数は最大 2^m である．

Proof. 2-伝播基底集合 $\{b_i\}$ に $2^m + 1$ 以上の元が存在

した場合，$b_i^{(0)} = b_j^{(0)}$ となるベクトルが存在する．このとき基底の和 $b_i + b_j$ を考えると $(b_i + b_j)^{(0)}$ はゼロベクトルであり定義である「$(b_i + b_j)$ は $\mathbb{Z}_2^m$ の基底である」という事実に反する．ゆえに $\mathbb{Z}_2^m$ 上の 2-伝播基底集合 $\{b_i\}$ の位数は高々 2^m である．∎

Definition14 (基底 b と基底行列 B) $\mathbb{Z}_2^m$ 上のベクトル集合 $b = b^{(1)}, b^{(2)}, \ldots, b^{(m)}$ に対して行ベクトルで構成された $m \times m$ 行列 B について，実数上の行列と同様に行列の階数 $(rank)$ を定義可能である．つまり線形独立な行ベクトルの個数を $rank(B)$ と記載する．

Remark15 2-伝播基底集合 $\{b_i\}$ の各基底に対する基底行列を $\{B_i\}$ とすると，$rank(B_1) = 0$ （b_1 はゼロベクトルの集合のため），$rank(B_i) = m (i = 2, \ldots, l)$, $rank(B_i + B_j) = m (i, j = 1, \ldots, l)$（ただし $i \neq j$）を満たす．

Theorem16 2-伝播基底集合 $\{b_i\}$ が存在すれば，任意の $\alpha_i \in \mathbb{Z}_2$ に対する $\sum_{i=1}^m \alpha_i b_i$ も 2-伝播基底集合 $\{b_i\}$ に含むことができる．

Proof. 2-伝播基底集合 $\{b_i\}$ の各基底に対する基底行列を $\{B_i\}$ とする．このとき，任意の $\alpha_i \in \mathbb{Z}_2$ に対して $rank(\sum_{i=1}^m \alpha_i Bi) = m$ であることを示せばよい．基底行列 B_i に対して 基底行列 B_j を足す操作は行列の $rank$ が変わらないことから行列への基本操作が行われている，すなわち B_i に対して両側から行列が掛けられていることを意味する．つまり $B_i + B_j = L_j B_i R_j$ となる 2 行列 L_j, R_j が存在する．一方で $B_j + B_i = L_i B_j R_i$ を満たす． $B_i + B_j = B_j + B_i$ であることから式変形を行うと $B_i = (L_j^{-1} L_i) B_j (R_i R_j^{-1})$ となり $B_i = L' B_j R'$ となる 2 行列 L', R' が存在する．よって $\sum_{i=1}^m \alpha_i B_i = B_{i_1} + B_{i_2} + \ldots, B_{i_t} = L_{i_2} B_{i_1} R_{i_2} + B_{i_3} + \ldots + B_{i_t} = \ldots = L B_{i_1} R$ となる 2 行列 L, R が存在し $rank(B_{i_1}) = m$ であることが分かる．∎

Lemma17 $\mathbb{Z}_2^m$ 上の 2-伝播基底集合 $\{b_i\}$ の位数は 2^t という形となる．2-伝播基底集合 $\{b_i\}$ の中に t 個の生成基底 $\{c_i\} (i = 1, \ldots, t)$ を持ち各基底 b_i はこれらで張られるベクトル空間の元，つまり $b_i = \sum_{j=1}^t \alpha_j c_j$ を満たす．

Remark18 $\mathbb{Z}_2^m$ 上の 2-伝播基底集合 $\{b_i\}$ の位数が 2^m の optimal な場合, 任意の j に対して $\{b_i^{(j)}\} (i = 1, \ldots, 2^m)$ はすべて異なるベクトルで構成される．

4.2 XOR-$(2, 2^m)$-SSS の構成

前節で定義した $\mathbb{Z}_2^m$ 上の 2-伝播基底集合 $\{b_i\}$ から XOR-$(2, 2^m)$-SSS を構成することを示す．

Theorem19 (Main Theorem) optimal な $\mathbb{Z}_2^m$ 上の 2-伝播基底集合 $\{b_i\} (i = 1, \ldots, 2^m)$ が存在するとき，ベクトル表現 $\{w_{ij} = b_i^j\} (i = 1, \ldots, 2^m, i = 1, \ldots, m)$ を持つ XOR-$(2, 2^m)$-SSS が存在する．

Proof. 2-伝播基底集合の定義から任意の異なる u, v に対して $b_u + b_v$ もまた基底となるため $w_1^* = w_{u1} + w_{v1}, \ldots, w_m^* = w_{um} + w_{vm}$ は $\mathbb{Z}_2^m$ 上の基底となる．相異なる 2 つのサブシェアの XOR 和 $W_u \oplus W_v$ の 第 l 成分は $\bigoplus_{s=1}^m w_l^{*(s)} M_s$ となる．ここで M_s に対する独立した連立方程式が m 個存在することになり $M_s (s = 1, \ldots, m)$ の全てを復元できることを意味する．∎

5. 2-伝播基底集合の存在性について

Theorem19 に示したように optimal な $\mathbb{Z}_2^m$ 上の 2-伝播基底集合 $\{b_i\} (i = 1, \ldots, 2^m)$ の存在性を示せば XOR-$(2, 2^m)$-SSS が存在することがわかる．本章では Theorem13 に示されるように最大位数 2^m となる 2-伝播基底集合の存在性について扱う．

5.1 小さい m に対する存在性確認シミュレーション

以下のようなプログラムを用いて存在性について確認を行った．

プログラム.

(1) set $m > 1$ （次元を一意に決定）
(2) set $b_1 := \{(0, \ldots, 0), \ldots, (0, \ldots, 0)\}$（m 次元ゼロベクトルを m 個並べたもの）
(3) set $b_2 := \{(1, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 1)\}$（m 次元正規ベクトルを m 個並べたもの）
(4) set c:= 3
(5) ${b_c}^R \in (\mathbb{Z}_2^m)^m$, check $rank(B_c + B_i) =?= m$ for all $i = 1, \ldots, c-1$
(6) if YES then add b_c into $\{b_i\}$, set $c = c++$
(7) if NO then return (5)

5.2 具体的構成例

以下小さい位数における具体的構成例について示す．W_0 は ゼロベクトル基底に呼応し，$W_1, \ldots, W_m$ は Lemma17 の生成基底 c_i に対応する．全シェアは Theorem19 に記載の $\bigoplus_{s=1}^m w_l^{*(s)} M_s$ で構成される．

Example20 ($m = 3$: XOR-$(2, 2^3)$-SSS)

W_0	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$
W_1	$(1,0,0)$	$(0,1,0)$	$(0,0,1)$
W_2	$(0,1,1)$	$(1,0,0)$	$(0,1,0)$
W_3	$(1,1,0)$	$(0,1,1)$	$(1,0,0)$

Example21 ($m = 4$: XOR-$(2, 2^4)$-SSS)

W_0	$(0,0,0,0)$	$(0,0,0,0)$	$(0,0,0,0)$	$(0,0,0,0)$
W_1	$(1,0,0,0)$	$(0,1,0,0)$	$(0,0,1,0)$	$(0,0,0,1)$
W_2	$(1,1,0,0)$	$(1,0,0,0)$	$(0,0,1,1)$	$(0,0,1,0)$
W_3	$(0,0,1,1)$	$(1,0,0,1)$	$(0,1,1,0)$	$(0,1,0,0)$
W_4	$(0,1,0,1)$	$(0,1,1,0)$	$(1,1,0,0)$	$(1,0,0,0)$

Example22 ($m = 5$: XOR-$(2, 2^5)$-SSS)

W_0	(0, 0, 0, 0, 0)	(0, 0, 0, 0, 0)	(0, 0, 0, 0, 0)	(0, 0, 0, 0, 0)	(0, 0, 0, 0, 0)
W_1	(1, 0, 0, 0, 0)	(0, 1, 0, 0, 0)	(0, 0, 1, 0, 0)	(0, 0, 0, 1, 0)	(0, 0, 0, 0, 1)
W_2	(0, 0, 1, 0, 0)	(1, 0, 0, 0, 0)	(0, 1, 0, 0, 0)	(0, 0, 0, 1, 1)	(0, 0, 0, 1, 0)
W_3	(1, 1, 0, 0, 0)	(1, 0, 0, 0, 1)	(0, 0, 0, 1, 1)	(0, 0, 1, 1, 0)	(0, 0, 1, 0, 0)
W_4	(0, 0, 0, 1, 0)	(0, 0, 0, 1, 1)	(1, 0, 0, 0, 0)	(0, 1, 1, 0, 0)	(0, 1, 0, 0, 0)
W_5	(0, 1, 1, 1, 1)	(0, 1, 1, 0, 0)	(0, 0, 0, 0, 1)	(1, 0, 1, 0, 1)	(1, 0, 0, 0, 0)

Example23 ($m = 6$: XOR-$(2, 2^6)$-SSS)

W_0	(0, 0, 0, 0, 0, 0)	(0, 0, 0, 0, 0, 0)	(0, 0, 0, 0, 0, 0)
W_1	(1, 0, 0, 0, 0, 0)	(0, 1, 0, 0, 0, 0)	(0, 0, 1, 0, 0, 0)
W_2	(0, 0, 0, 0, 0, 1)	(1, 0, 0, 0, 0, 1)	(0, 1, 0, 0, 0, 0)
W_3	(0, 0, 0, 0, 1, 0)	(0, 0, 1, 0, 0, 0)	(1, 0, 0, 0, 0, 0)
W_4	(0, 0, 0, 1, 0, 1)	(1, 0, 0, 0, 1, 1)	(1, 1, 0, 0, 0, 1)
W_5	(0, 0, 1, 0, 1, 0)	(0, 0, 1, 1, 0, 0)	(0, 0, 1, 0, 1, 1)
W_6	(0, 1, 0, 0, 0, 1)	(0, 1, 1, 1, 0, 1)	(1, 0, 1, 1, 0, 1)
W_0	(0, 0, 0, 0, 0, 0)	(0, 0, 0, 0, 0, 0)	(0, 0, 0, 0, 0, 0)
W_1	(0, 0, 0, 1, 0, 0)	(0, 0, 0, 0, 1, 0)	(0, 0, 0, 0, 0, 1)
W_2	(0, 0, 1, 0, 0, 0)	(0, 0, 0, 1, 0, 0)	(0, 0, 0, 0, 1, 0)
W_3	(0, 1, 0, 0, 0, 0)	(0, 0, 0, 0, 1, 1)	(0, 0, 0, 1, 0, 0)
W_4	(0, 1, 0, 0, 0, 1)	(0, 0, 1, 0, 0, 1)	(0, 0, 1, 0, 0, 0)
W_5	(1, 0, 0, 0, 0, 0)	(0, 1, 0, 0, 1, 0)	(0, 1, 0, 0, 0, 0)
W_6	(0, 1, 0, 0, 1, 0)	(1, 0, 0, 1, 0, 0)	(1, 0, 0, 0, 0, 0)

予測. 任意の素数 p に対して XOR-$(2, p)$-SSS の存在性が示されていることから，optimal な $\mathbb{Z}_2^p$ 上の 2-伝播基底集合 $\{b_i\}$ $(i = 1, \ldots, p^2)$ の一般的構成方式が存在すると考えられる．

一方で XOR-$(2, 2^m)$-SSS の利用用途を考えると XOR-$(2, 2^6)$-SSS まで存在性が示されていれば十分とも考えられる．

6. まとめ

$\mathbb{Z}_2^m$ 上の基底集合に対して 2-伝播基底集合を定義し，排他的論理和を用いた $(2, 2^m)$-閾値秘密分散法の新しい構成について提案した．2-伝播基底集合についての一般的な構成法や存在性については未解決問題である．そこで本稿では小さい m については探索アルゴリズムを実装しその存在性および XOR-$(2, 2^m)$-SSS の存在性について明らかにした．

XOR-$(2, 2^m)$-SSS 構成に関して，既存方式と比べた分割時・復元時の効率性の評価についてはパラメータに大きく依存しケースバイケースであり，選択するシェアによっては大きく異なると考えられる．最悪時・中間値などについて計算量の理論的な見積りとシミュレーションによる結果については今後の課題とする．

また $k > 2$ に対する XOR-$(k, 2^m)$-SSS への自然な拡張を今後検討する．容易であると考えられるナイーブな拡張方法では乱数ブロックの差し込み方がエレガントではないため，現時点ではその構成法に関する記載は行っていないが，改良案が構成でき次第別途報告したい．

参考文献

[1] Open Cloud Manifesto, http://www.opencloudmanifesto.org/
[2] Open Cloud Consortium, http://www.opencloudconsortium.org/
[3] Cloud Security Alliance, http://www.cloudsecurityalliance.org/
[4] DMTF's Open Cloud Standards Incubator, http://www.dmtf.org/standards/cloud
[5] NIST's definition of cloud computing, http://csrc.nist.gov/groups/SNS/cloud-computing/
[6] http://www.opencloudmanifesto.org/opencloudmanifesto2.htm
[7] 須賀, "クラウド時代のセキュリティ確保とプライバシ保護を実現する暗号プロトコル技術", NICT 情報通信セキュリティシンポジウム, 2010.
[8] IIJ, IIR vol.4, 1.4.3 "クラウドコンピューティングとセキュリティ", http://www.iij.ad.jp/development/iir/pdf/iir_vol04_infra.pdf
[9] グローバルクラウド基盤連携技術フォーラム, http://www.gictf.jp/
[10] OASIS Identity In the Clouds TC, http://www.oasis-open.org/committees/id-cloud/charter.php
[11] SAS 70 type II, http://www.sas70.com/
[12] FMMC, ASP・SaaS 安全・信頼性情報開示認定制度, http://www.fmmc.or.jp/asp-nintei/
[13] 経済産業省, "SaaS 向け SLA ガイドライン"
[14] C.C.Aggarwal and P.S.Yu "Privacy-Preserving Data Mining: Models and Algorithms", Advances in Database Systems Series, Springer-Verlag, 2008.
[15] Hakan Hacigumus, Hakan Hacg Um Us, Bala Iyer, Chen Li,Sharad Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model", SIGMOD02, pp.216-227
[16] Craig Gentry, "Fully homomorphic encryption using ideal lattices", Annual ACM Symposium on Theory of Computing, 2009.
[17] Damien Stehle, Ron Steinfeld, "Faster Fully Homomorphic Encryption", ASIACRYPT2010.
[18] Okamoto, Takashima, "Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption", CRYPTO 2010, pp.191-208.
[19] Shamir Adi, "How to share a secret", Communications of the ACM 22 (11): 612-613, 1979
[20] http://www.nri-secure.co.jp/news/2010/0113.html
[21] http://www.unisys.co.jp/club/closeup/no22.html
[22] 藤井, 多田, 保坂, 栃窪, 加藤, 高速な (2, n) 閾値法の構成法とシステムへの応用, 8C-2, CSS2005.
[23] 多田, 藤井, 保坂, 栃窪, 加藤, 閾値 3 の秘密分散法の構成法, 8C-3, CSS2005.
[24] 藤井, 栃窪, 保坂, 多田, 加藤, 排他的論理和を用いた (k,n) しきい値法の構成法, ISEC2007-05.
[25] 栗原, 清本, 福島, 田中, 排他的論理和を用いた高速な (4,n) 閾値秘密分散法と (k,n) 閾値法への拡張, ISEC2007-04.
[26] J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, On a fast (k, n)-threshold secret sharing scheme, IEICE Trans. Fundamentals, vol.91-A, no.9, Sep. 2008.
[27] 須賀, 排他的論理和を用いた (k,n) 閾値秘密分散法の新しい構成とその優位性について, 1C2-4, CSS2012.