5ZC-07

シェアの再分配なしにアクセス構造を更新可能な完全な (k, n) しきい値秘密分散法の安全性評価

相澤　直樹†　　栃窪　孝也‡

日本大学大学院生産工学研究科数理情報工学専攻†　　日本大学生産工学部数理情報工学科‡

１．はじめに

秘密分散法の一方式である (k, n) しきい値法[1]は、秘密情報をシェアと呼ばれる n 個の断片情報に分割し、k 個以上のシェアから秘密情報を復元することができるが、$k-1$ 個以下だと秘密情報を復元することができない秘密情報の分散管理に有効な手法である。ただし、初期にシェアの配布を行った後、時間経過によって復元前にしきい値や管理者数等のアクセス構造を更新する必要が生じる場合がある。このような場合、一番簡易な解決法は、新しいシェアを再配布することであるが、常に安全な通信路が確保されていることが前提であり現実的でない。1999 年に田村らはブロードキャストを用いた再配布なしでアクセス構造を更新する手法(以下 TCSS)を提案した[2]。また、2001 年に Keith らは、田村らの手法が更新する際の条件によっては安全性に脆弱性があることを指摘しているが、その検証は限定的であり不十分である[3]。

本稿では、より大きな素体や管理者数に対して Keith らの攻撃手法を適用し、その安全性を厳密に評価する。

２．秘密分散法

秘密を s とし、s を n 個のシェア $v_1, \ldots, v_n$ に分割する。$\boldsymbol{P} = \{P_1, \ldots, P_n\}$ を n 人のシェアの管理者集合とする。管理者 P_i にシェアを配布する者をディーラー(以下 D)とすると、有限体 K 上での (k, n) しきい値法は次の手順で構成される。

分散段階：

(1) D は、$a_1, \cdots, a_{k-1} \in K$ をランダムに選び、秘密を $s \in K$ とし、以下の式のような有限体上の $k-1$ 次の多項式を作成する。

$$f(x) = s + \sum_{l=1}^{k-1} a_l x^l \in K$$

(2) 秘密でない互いに異なる非零の要素を $x_1, \ldots, x_n \in K$ として、D はシェア $v_i = f(x_i)$ を計算し、P_i に v_i を送信する $(1 \le i \le n)$。

復元段階：

秘密の復元者は n 人のうち k 人の管理者 $P_{i_1}, \cdots, P_{i_k}$ から x_i を含むシェアのペア $(x_{i_1}, v_{i_1}), \cdots, (x_{i_k}, v_{i_k})$ を受け取った後、$f(x)$ を求めることで $s(= f(0))$ を復元する。一方、$k-1$ 個以下では復元することができない。

本稿では K に、素数を q とした素体 $\mathbb{Z}_q$ を用いる。

３．田村らの TCSS

田村らの TCSS は条件として、しきい値の更新前後で秘密の変更を要し、通常の (k, n) しきい値法と異なり各管理者の値 x_i $(1 \le i \le n)$ を常に秘匿する。しきい値の更新時には、管理者全員のシェアを利用するため、更新者は少なくとも k 人分のシェアと管理者 n 人分の x_i $(1 \le i \le n)$ を保持している必要がある。更新は一度のみ実行され、秘密 s における (k, n) しきい値法に対し、更新後の秘密を $s'(s' \ne s)$、更新後のしきい値を $k'(k < k' \le n)$ とした場合を考える。

(1) 新しい秘密の点 $(0, s')$ を含む $(n+1)$ 個の座標点で決まる一意の n 次多項式の係数 b_j $(1 \le j \le n)$ を以下の行列の連立方程式を用いて求める。

$$\begin{bmatrix} x_1 & x_1^2 & \cdots & x_1^n \\ x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & \vdots & \ddots & \vdots \\ x_n & x_n^2 & \cdots & x_n^n \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} f(x_1) - s' \\ f(x_2) - s' \\ \vdots \\ f(x_n) - s' \end{bmatrix}$$

(2) n 次多項式 $g(x) = s' + \sum_{j=1}^{n} b_j x^j$ $(1 \le j \le n)$ を定める。

(3) 新たに生成された $g(x)$ は n 次多項式なので、係数 b_j $(k' \le j \le n)$ を管理者にブロードキャストすることにより $g(x)$ は未知の係数が秘密 s' を含め k' 個となり、しきい値を k' に変更することができる。

４．Keith らの攻撃手法

$(x_i, f(x_i))$, $(1 \le i \le k)$ を知っている k 人の管理者集合が s' を解読する場合を考える。$h(x) = g(x) - f(x)$ とすると $h(x)$ は n 次多項式であり、$h(x) = 0$ となる値 x は最大で n 個存在し、各管理者の x_i は $h(x_i) = 0$ $(1 \le i \le n)$ となる唯一の解となるため、$\lambda \in \mathbb{Z}_q$ を用いて $h(x) = \lambda(x - x_1)(x - x_2) \cdots (x - x_n)$ と表すことができる。よって $h(0) \ne 0$ であり $s' \ne s$ が成り立つ。攻撃者は、n 個の因数において相異なる非零の解 x_i を持つ n 次多項式の候補を探索するこ

Security Evaluation on Perfect Threshold Changeable Secret Sharing Schemes
†Naoki Aizawa, Nihon University
‡Kouya Tochikubo, Nihon University

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.

表 1 初期が$\mathbb{Z}_{19}$上の$(2,7)$しきい値法、s =1、s' =2 の場合にしきい値をk'に増加させた時の結果

k'	$e(\alpha)$	$a(\alpha)$	候補となる多項式の数																		
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
3	0.002	0.05	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0.03	0.11	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0.64	0.63	0	0	3	1	2	1	0	0	2	1	0	0	0	0	0	1	0	1	0
6	12.10	12.00	12	0	13	14	12	13	15	10	16	12	13	12	14	13	11	14	11	11	12

表 2 初期が$\mathbb{Z}_{19}$上の$(2,8)$しきい値法、s =1、s' =2、の場合にしきい値をk'に増加させた時の結果

k'	$e(\alpha)$	$a(\alpha)$	候補となる多項式の数																		
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
3	0.0002	0.05	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0.0032	0.05	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0.06	0.11	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	1.17	1.26	2	0	2	1	3	2	1	2	3	1	1	0	0	0	2	3	0	1	0

表 3 初期が$\mathbb{Z}_{31}$上の$(2,6)$しきい値法、s =1、s' =2、の場合にしきい値をk'に増加させた時の結果

k'	$e(\alpha)$	$a(\alpha)$	候補となる多項式の数																												
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
3	0.03	0.11	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0.92	1.05	1	0	2	2	0	1	2	1	0	0	0	0	0	0	0	0	0	0	1	0	0	2	0	0	0	0	2	3	1	1	1
5	28.52	34.74	19	0	21	22	20	26	22	24	20	21	24	21	22	22	22	18	16	25	22	25	23	23	25	21	23	23	19	22	24	22	23

とで$h(x)$を決定しようとするが、k人の攻撃者が持つx_i $(1 \le i \le k)$は既知であるため、$h(x)$の可能性がある多項式候補群$h_{\gamma_1}(x)$は$\alpha_j \in \mathbb{Z}_q \setminus \{0, x_1, \dots, x_k\}, (1 \le j \le n-k)$を用いて以下のように表される。

$$h_{\gamma_1}(x) = \lambda(x-x_1)(x-x_2)\cdots(x-x_k)(x-\alpha_1)\cdots \cdots(x-\alpha_{n-k})$$

また、$h(x)$のk次からn次の係数は$g(x)$と一致し、ブロードキャスト済み係数b_i $(k' \le i \le n)$ は既知より、$q^{k'}$個の$h(x)$の可能性がある多項式候補群$h_{\gamma_2}(x)$は$\beta_i \in \mathbb{Z}_q (0 \le i \le k'-1)$を用いて以下で表される。

$$h_{\gamma_2}(x) = \beta_0 + \cdots + \beta_{k'-1}x^{k'-1} + b_{k'}x^{k'} + \cdots + b_n x^n$$

これを前述した一方の多項式候補群$h_{\gamma_1}(x)$と比較することで$h(x)$候補を絞り込み、かつ$h(0) = \beta_0 = s' - s$から、更新前の秘密sはk人にとって既知なので、更新後の秘密s'の候補を絞り込むことができる。また、攻撃者は事前に候補となる多項式$h(x)$の数の期待値$e(\alpha) = \binom{q-k-1}{n-k} / q^{n-k'+1}$を概算することで有効性を予測することができる。

5．評価

$(2, n)$しきい値法を、$s = 1$, $a_1 = 2$, $\{x_1, \dots, x_n\} = \{1, \dots, n\}$とするとき、$s' = 2$として$\mathbb{Z}_q$または$n$が可変の下、$x_1 = 1, x_2 = 2$を持つ管理者$P_1, P_2$が共謀して$k'$が異なる田村らの TCSS に Keith らの攻撃手法を適用した結果を表$1, 2, 3$に示す。s'候補の列は、s'と成り得る$\mathbb{Z}_q$のすべての要素において、計算機によって絞り込まれた各s'候補の値が導き出される$h(x)$の多項式候補の数を表しており、$a(\alpha)$は結果より得られるその平均出現頻度を表している。いずれも$a(\alpha) < 1$の場合に Keith らの攻撃手法は極めて有効であり、秘密s'を一意、あるいはかなり限定することができる。また、管理者数nの値が大きいほどs'の推測が困難になるまでより大きなk'を要することがわかる。さらに、[3]の検証結果と比較して素数qの増加は安全性の向上に有効であることがわかった。

謝辞　本研究はJSPS科研費21K11893の助成を受けたものです。

参考文献

[1] Adi Shamir, “How to share a secret,” Communications of the ACM, Vol.22, No.11, pp.612-613, 1979.

[2] Y. Tamura, M. Tada and E. Okamoto, “Update of access structure in Shamir’s (k, n) threshold scheme,” Proceedings of The 1999 Symposium on Cryptography and Information Security, vol.1, pp.469-474, 1999.

[3] K.M. Martin, J. Nakahara Jr, “Weakness of protocols for updating the parameters of an established threshold scheme,” IEE Proceedings Computers and and Digital Techniques, Vol.148, No.1, pp.45-48, 2001.

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.