高速な({1,3},n)階層的秘密分散法の研究

Studies on fast ({1,3},n) hierarchical secret sharing schemes

島 幸司・ネットワーク分科会・情報セキュリティ大学院大学

Abstract We look at hierarchical secret sharing schemes in the purpose of the ease of deleting the secret, and apply a hierarchical secret sharing scheme to Fujii et al.'s method of using XOR. Also, we inherit Tassa's idea of using derivatives and Birkhoff interpolation, and propose a ({1,3},n) hierarchical secret sharing scheme considering applying to finite fields of characteristic 2.
Our implementation system on a PC with Intel Celeron G1820 2.70GHz and 3.6GB RAM can recover the secret in the processing of around 970Mbps.

階層的秘密分散法：最小限の高いレベルの参加者が必要とされる秘密分散法
例：金庫を開けるには3人の従業員が必要で少なくとも1人は部長というシナリオ.
秘密消去の容易性がある(秘密情報の消去が必須参加者のシェア削除で保証されるため).

提案１：藤井らの(2,n)しきい値法を拡張した({1,3},n)階層的秘密分散法

藤井らの方式における秘密情報の断片を乱数$R_0, \dots, R_4$に置き換え，$w_0, \dots, w_4$を生成し，それらの必要なw_iに秘密情報sを混ぜてシェア$W_0, \dots, W_4$を配布する.

$$W_0 = w_0 \oplus s$$
$$W_1 = w_1 \oplus s$$
$$W_2 = w_2$$
$$W_3 = w_3$$
$$W_4 = w_4$$

⇦

w_0	r_0	$R_4 \oplus r_1$	$R_3 \oplus r_2$	$R_2 \oplus r_3$
w_1	$R_1 \oplus r_0$	r_1	$R_4 \oplus r_2$	$R_3 \oplus r_3$
w_2	$R_2 \oplus r_0$	$R_1 \oplus r_1$	r_2	$R_4 \oplus r_3$
w_3	$R_3 \oplus r_0$	$R_2 \oplus r_1$	$R_1 \oplus r_2$	r_3
w_4	$R_4 \oplus r_0$	$R_3 \oplus r_1$	$R_2 \oplus r_2$	$R_1 \oplus r_3$

提案２：導関数の標数2の有限体上への適用を考慮した({1,3},n)階層的秘密分散法

Tassaのアイデアを継承し，試行錯誤を経て次の結論に到達した.

試行錯誤１：標数2の有限体上への適用に工夫が必要とわかる.
標数2の有限体上で微分すると，次数が偶数の項は消えてしまう．☹
2次多項式$f(x) = 3x^2 + 5x + 7$について$f'(x) = 5$.

試行錯誤２：3次多項式をランダムに選び，必須参加者に相当する1つのシェアをグローバルに共有.
うまく動作した！ ☺
$(\{1,k\},n)$階層的秘密分散法への一般化ができない．ストレージ面で優位性がない．☹

試行錯誤３：2変数を持つ多項式に $\mathcal{G} = \{1, x, x^3\}$ として Birkhoff補間を適用する.
うまく動作し，高速化もできた！ ☺/
$f(X) = a_2X^3 + a_1X + s \in \mathrm{GF}(2^l)$をランダムに選び，必須参加者1人を含む3人が復元に協力し，
$f(x_1) = a, f'(x_2) = b, f'(x_3) = c$とすると，

$$s = f(0) = \frac{D(E, X, \mathcal{G}_0)}{D(E, X, \mathcal{G})} = \frac{a(x_2^2 + x_3^2) + bx_1(x_1^2 + x_3^2) + cx_1(x_1^2 + x_2^2)}{x_2^2 + x_3^2}.$$