【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成18年9月21日(2006.9.21)

【公開番号】特開2005-303776(P2005-303776A)
【公開日】平成17年10月27日(2005.10.27)
【年通号数】公開・登録公報2005-042
【出願番号】特願2004-118706(P2004-118706)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ａ

【手続補正書】
【提出日】平成18年8月8日(2006.8.8)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
（ｋ，ｎ）閾値秘密分散法は、分散情報を配布する数である２以上の整数の分散数ｎと、秘密情報Ｓの復元に必要な分散情報の最低数である２以上ｎ以下の整数の閾値ｋから、秘密情報Ｓを定数項とする（ｋ－１）次の多項式ｆ（ｘ）を、
$$f(x)=S+R_1x+\cdots+R_{k-1}x^{k-1} \mod P \quad \cdots(1)$$
として作成し（R_1，…，R_{k-1}：乱数、Ｐ：素数）、元の秘密情報Ｓを所有あるいは預託により分配する秘密情報分配者は、分散情報を保管する各分散情報保持者ｉ（ｉ＝１，２，…，ｎ）に対して、分散情報Ｗｉ＝ｆ（ｉ）を分配するものである。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１４
【補正方法】変更
【補正の内容】
【００１４】
（ｄ，ｋ，ｎ）閾値秘密分散法は、上記（ｋ，ｎ）閾値秘密分散法を拡張したもので、分散情報を配布する数である２以上の整数の分散数ｎと、秘密情報Ｓの完全な復元に必要な分散情報の最低数である２以上ｎ以下の整数の閾値ｋと、閾値ｋに対して秘密情報Ｓの部分的な復元を許容する分散情報の不足数を決定する２以上ｋ以下の整数の分割数ｄから、秘密情報ＳをS_0，S_1，…，S_{d-1}に分割し、これらの分割した秘密情報（分割情報）を定数項とする（ｋ－１）次の多項式ｆ（ｘ）を、
$$f(x)=S_0+S_1x+\cdots S_{d-1}x^{d-1}+R_1x^d+\cdots+R_{k-d}x^{k-1} \mod P \quad \cdots(2)$$
として作成し（R_1，…，R_{k-1}：乱数、ｐ：素数）、元の秘密情報Ｓを所有あるいは預託により分配する秘密情報分配者は、分散情報を保管する各分散情報保持者ｉ（１＝１，２，…，ｎ）に対して、分散情報W_i＝ｆ（ｉ）を分配するものである。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正の内容】

【００１８】
この復元制御型秘密情報分散法は、基本的には、秘密情報Ｓについて、秘密情報Ｓの完全な復元に必要な分散情報の最低数である２以上の整数の閾値ｋ、閾値ｋに対して秘密情報Ｓの部分的な復元を許容する分散情報の不足数を決定する２以上ｋ以下の整数の分割数ｄと、秘密情報Ｓのｄ個の分割情報（分配情報）S_0，S_1，…，S_{d-1}などの秘密情報Ｓを分散するための条件を入力し、
最大の分割情報S_t（０≦ｔ≦ｄ－１）よりも大きな素数Ｐと、素数Ｐよりも小さく０でない（ｋ－ｄ個）の乱数R_i（１≦１≦ｋ－ｄ）と、（ｋ（ｋ－１）／２）個の乱数a_j（１≦ｊ≦ｋ（ｋ－１）／２）を生成して、

$$f(x)=S_0+S_1(x-a_1)+\cdots+S_{d-1}(x-a_{(d-1)(d-2)/2+1})(x-a_{(d-1)(d-2)/2+2})\cdots(x-a_{(d-1)(d-2)/2+d-1})+R_1(x-a_{d(d-1)/2+1})(x-a_{d(d-1)/2+2})\cdots(x-a_{d(d-1)/2+d})+\cdots+R_{k-d}(x-a_{(k-1)(k-2)/2+1})(x-a_{(k-1)(k-2)/2+2})\cdots(x-a_{(k-1)(k-2)/2+k-1}) \mod P \quad \cdots(3)$$

の式で表現される秘密情報Ｓの分散関数ｆ（ｘ）を生成するものである。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】変更
【補正の内容】
【００１９】
上記式（３）の分散関数ｆ（ｘ）は、例えばｋ＝３、ｄ＝２とした場合、

$$f(x)=S_0+S_1(x-a_1)+r(X-a_2)(x-a_3) \mod P \quad \cdots(4)$$

で表現され、任意の２個の分散情報W_xとW_{x+b}についての連立方程式は以下のような行列式で表現できる。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】変更
【補正の内容】
【００２０】
【数１】

$$\begin{bmatrix}1 & x-a_1 & (x-a_2)(x-a_3)\\ 1 & x+b-a_1 & (x+b-a_2)(x+b-a_3)\end{bmatrix}\begin{bmatrix}S_0\\ S_1\\ r\end{bmatrix}\equiv\begin{bmatrix}W_x\\ W_{x+b}\end{bmatrix} \quad \cdots(5)$$

上記行列式の左項を掃き出し法により変形すると、
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正の内容】
【００２１】

【数２】

$$\begin{bmatrix} 1 & 0 & -x^2+(2a_1-b)x+a_1b-a_1a_2-a_1a_3+a_2a_3 \\ 0 & 1 & 2x+b-a_2-a_3 \end{bmatrix} \quad \cdots (6)$$

となり、ａ１，ａ２，ａ３の値によっては－ｘ２＋（２ａ１－ｂ）ｘ＋ａ１ｂ－ａ１ａ２－ａ１ａ３＋ａ２ａ３≡０，もしくは２ｘ＋ｂ－ａ２－ａ３≡０を満たすｘとｂがある場合に、連立方程式から分割情報（部分情報）のＳ０のみ、もしくはＳ１のみを求めることができる。