通信情報保護學會論文誌
第 7 卷 第 4 號, 1997. 12

비밀분산방식의 새로운 구성법

송 유 진*

New Construction of Secret Sharing Scheme

Youjin Song

요 약

본 논문은 기존 비밀분산방식의 악세스 구조를 조합디자인 이론의 관점에서 해석함으로써 새로운 비밀분산방식이 구성될 수 있음을 보인다. 종래의 비밀분산방식으로서는 다항식보간을 이용하는 방법, 사영기하를 이용하는 방법등이 알려져 있으나 본 논문에서는 OA(Orthogonal Arrary), t-(v,k,1) 디자인, 그룹분할 가능한GD(Group Divisible) 디자인이 갖는 행렬구조로부터 비밀분산방식의 악세스 구조를 정합시킴으로써 비밀분산방식을 새롭게 구성하고 있다. 이와같이 구성된 비밀분산방식은 기존 방식의 비밀 사이즈가 소수의 멱승 q에 의존하고 있는 반면 본 방식의 경우 조합디자인 파라메터에 관계하고 있으므로 비밀 사이즈 선택의 융통성이 있고 잘 알려진 조합적 구조를 이용함으로써 실현이 용이한 특징을 갖는다.

키워드 : 비밀분산방식, OA(Orthogonal Arrary), t-(v,k,1) 디자인, GD(Group Divisible) 디자인.

1. 서 론

비밀분산방식이란 비밀 s를 n개의 분산정보 $v_1, v_2, \ldots, v_n$으로 분산부호화하여 특정분산정보의 집합(악세스집합)에 대해서만 s의 복호를 가능토록 하는 방식이다. 이는 비밀정보의 관리뿐만 아니라 Multiparty프로토콜, 그룹암호계등의 많은 분야에서 중요하다. 비밀분산방식은 비밀 s의 난수 R를 입력으로 하고 $v_1, v_2, \ldots, v_n$를 출력으로 하는 알고리즘에 의해 실행된다. 비밀분산방식은 임의의 부분집합 A가 비밀 s를 완전히 복원할 수 있을까(A는 악세스집합), 비밀s에 관한 정보를 완전히 얻을 수 없을까(A는 비악세스집합)의 어느 쪽인가에 의해 비밀정보를 분산 관리하는 방식이다[1]. Shamir[13]는 비밀 분산 방식을 실현하는 체계적인 절차인 다항식보간을 이용한 (k, n)임계치법을 제안했다. 또한 Blakley[6]는 거의 동일

* 동국대학교 정보산업학과

한 시기에 독립적으로 사영기하를 이용한 (k, n) 임계치법을 제안하여 Shamir의 제안을 소수 p상의 유한체 $GF(p)$에서 $GF(2^n)$상의 원시 다항식 연산으로 확장하였다. Karnin, Greene, Hellman[11]은 최대 거리 부호의 성질을 비밀분산 방식에 적용하였고 Asmuth, Bloom[7]은 비밀분산방식에 대한 모듈로 접근법을 제안하였다. 그리고 McEliece, Sarwate[12]는 Shamir의 방식이 Reed-Solomon 부호와 매우 밀접하다는 것을 고찰하고 있다.

본 논문에서는 OA(Orthogonal Array), t-(v, k, l) 디자인, GD(Group Divisible) 디자인이 갖는 행렬구조로부터 비밀분산방식의 악세스 구조를 정합시킴으로써 비밀분산방식을 새롭게 구성하고 있다. 이와같이 구성된 비밀분산방식은 기존 방식의 비밀 사이즈가 소수의 멱승 q에 의존하고 있는 반면 본 방식의 경우 조합 디자인 파라메터에 관계하고 있으므로 비밀 사이즈 선택의 융통성이 있고 잘 알려진 조합적 구조를 이용함으로써 실현이 용이한 특징을 갖는다.

2. 기존 비밀 분산 방식의 구성법

본 장에서는 비밀분산방식에 대한 기존의 여러가지 구성법에 대하여 검토한다.

Shamir[13]는 Lagrange 보간 다항식을 근거로 한 방식을 제안했다. 분산정보 (Share)는 다음의 t-1차의 다항식에 의해 주어진다.

$$h(x)=(a_{t-1}x^{t-1}+\ldots+a_1x+a_0) \bmod p$$

단, 여기서 정수치 $a_0=s$ 이다. 모든 계산은 유한체 $GF(p)$에서 행하고 P는 s, k보다 큰 소수로 한다. $h(x)$가 주어지면 비밀 s는 $s=h(0)$에 의해 계산할 수 있다. k개의 분산정보를 구하기 위해 k개의 값 $x_1\ldots x_k$에 대해서 각각 $h(x)$의 수치를 계산한다.

$$v_i=h(x_i) \qquad i\text{-}1\ldots k$$

즉, 각각의 쌍 (x_i, v_i)는 곡선 $h(x)$상의 점으로써 주어진다.

수치 $x_1\ldots x_k$는 비밀로 할 필요는 없고 사용자의 식별번호 또는 단순히 1부터 k까지 번호라도 상관없다. t개의 점이 모여 비로소 t-1차의 다항식을 유일하게 결정할 수 있다. 따라서, t개의 분산정보는 $h(x)$ 즉 비밀 s를 복원할 수 있다.

한편, t미만의 분산정보에서는 $h(x)$및 s를 복원할 수 있는 정보를 얻을 수 없다. t개의 분산정보 v_1, v_2, ..., v_t가 주어지면, $h(x)$는 다음과 같은 Lagrange다항식으로부터 복원된다.

$$h(x)=\sum_{j=1}^{t} k_{is} \prod_{\substack{j=1 \\ j\neq s}} \frac{(x-x_{ij})}{(x_{is}-x_{ij})} \bmod p$$

Blakey[6]는 $p(x)=x^n+x+1$이 기약 다항식이라면 Shamir의 방식이 mod $p(x)$를 갖는 $GF(2^n)$상에서 보다 효율적으로 실현될 수 있음을 제안하였다. Blakley방식의 경우 $h(x)$의 계수 a_i는 $GF(2^n)$의 요소, 좌표(x_i, v_i)는 $GF(2^n)$의 요소이고 $h(x)$는 기약 mod $p(x)$이다.

Asmuth, Bloom[7]은 중국인 잉여정리에 근거한 비밀 분산 방식을 제안했다.

이 방식에서 분산정보는 비밀 s에 관한 수의 합동(congruence) 클래스로 된다.

Asmuth, Bloom의 비밀분산방식을 설명하기 위해 $\{p, d_1, d_2, \ldots d_k\}$를 다음 조건을 만족하는 정수의 집합으로 한다. 즉,

① $p>s$
② $d_1<d_2<\ldots<d_k$
③ 모든 i에 대해, gcd$(p, d_i)=1$
④ $i\neq j$ 일때 gcd$(di, dj)=1$
⑤ $d_1, d_2\ldots d_t>pd_{k-t+2}d_{k-t+3}\ldots d_k$

여기서, gcd(x, y)는 x와 y의 최대공약수를 나타낸다.

조건 ③, ④는 정수의 쌍이 쌍마다 서로소라는 것을 의미하며 조건 ⑤는 작은 쪽에서 t개를 취한 d_i의 곱은 큰 쪽의 나머지 t-1개의 d_i와 p의 곱보다 크다는 것을 의미한다.

$n=d_1d_2...d_t$를 작은 쪽으로 부터 t개의 d_i의 곱으로 한다.

이때 n/p은 나머지 t-1개의 d_i의 곱보다 크다.

r을 [0, (n/p-1)]의 범위에 있는 랜덤한 정수로 한다.

s를 k개의 분산정보로 분해하는 것은 $s'=s+rp$를 계산하는 것이다.

여기서 분산정보는

$$v_i=s' \bmod d_i \qquad i=1...k$$

에 의해 구해진다.

s를 복원하기 위해서 s'를 구하면 충분하다.

만약 t개의 분산정보 $v_1, v_2, \ldots, v_t$를 알고 있으면 s'는 중국인 잉여정리에 의해 구해진다. s'와 r, p로부터 $s=s'-rp$에 의해 s를 구한다.

본 논문은 이상과 전혀 다른 관점인 조합디자인 관점으로부터 비밀분산방식의 구성법을 검토한다. 즉, 본 논문은 Blakley[6]가 (k, n) 임계치법을 제안하기 위해 사용한 사영기하 $PG(2, 2)$의 구조는 2-(7, 3, 1)디자인이라는 점에 착안하여 비밀분산방식의 악세스 구조와 디자인 구조의 밀접한 관련성을 이용, 비밀분산방식을 제안하고 있다.

3. 조합 디자인에 근거한 비밀분산방식의 구성

본 장에서는 비밀분산방식의 악세스구조와 조합디자인이 갖는 조합적 구조와의 밀접한 관계에 대하여 고찰하고 조합디자인으로부터 비밀분산방식을 구성한다.

3.1 비밀분산방식과 조합디자인과의 관계

비밀에의 악세스 구조는 그래프 또는 매트로이드등의 조합적 구조에 의해 특징지워질 수 있음이 잘 알려져 있다[1][2][3][8][10][14]. 그래프 또는 매트로이드등의 조합적 구조는 비밀분산방식의 비밀복원특성(임의의 분산정보를 소유하는 멤버의 집합은 비밀을 복원할 수 있는 성질)을 형식화하기 위해 도입되고 있다.

이와같이 비밀분산방식은 BIBD(Balanced Incomplete Block Design), t-(v, k, 1)디자인등 균형성이 있는 부분집합의 족을 적절히 선택하여 비밀분산방식의 비밀복원특성을 만족하도록 할 수 있을까의 관점에서 해석할 수 있다. Shamir[13]의 (t, k) 임계치 방식은 t개의 점을 통하는 (t-1)차 다항식 f가 유일하게 존재한다는 성질을 이용하여 k명 중에 t명은 f를 결정할 수 있으므로 비밀을 복원하는 방식이다. 이는 t-(v, k, 1)디자인에서 k점중의 t개의 점이 주어지면 블록을 정확히 하나 결정할 수 있는 성질에 해당된다. 또한 Blakley[6]의 사영기하에 근거한 (t, k) 임계치 방식에서는 t개의 점으로부터 (t-1)차원 부분공간을 구성할 수 있는 것이 t-(v, k, 1)디자인적 성질에 해당되고 있다. 이와같이 t-(v, k, 1)디자인의 블록은 (t-1)차 다항식, (t-1)차원 부분공간등의 관점에서 해석할 수 있다.

여기서 본 논문에서 취급하는 조합디자인에 대하여 정의한다.

[정의 1][4][9] 직교배열 $OA_\lambda(t, k, n)$는 이하의 조건을 만족하는 $\lambda n_t \times k$ 배열 A이다.

(1) 배열 A의 요소는 $Z_n=\{0, 1, \ldots, n-1\}$중의 하나이다.

(2) 배열 A의 어떤 t열을 취해도 임의의 t조가 행으로서 λ회 나타난다.

[정의 2][4][9] t-(v, k, λ)디자인은 다음의 성질을 만족하는 v개의 점의 집합 X와 블록의 집합 D로 구성된다.

(1) 모든 블록은 정확히 k개의 점으로 구성된다.

(2) 임의의 t개의 점을 포함하는 블록의 개수는 정확히 λ개이다.

[정의 3][4][9] GD디자인 $GD(k, \lambda, n;v)$는 다음의 조건을 만족하는 v개의 점의 집합 X와 블록의 집합 D로 구성된다.

(1) 각 블록은 k개의 점으로 구성된다.

(2) $X=X_1\cup X_2\cup\ldots$라는 X의 분할이 존재하고 다음의 조건을 만족한다.

(2-1) 각 X_i의 요소 수는 n

(2-2) $\forall a\in X_i$, $\forall b\in X_j$에 대해서 $i=j$일때 (a, b)를 포함하는 블록은 존재하지 않는다.

(2-3) $i\neq j$일때 (a, b)를 포함하는 블록이 정확히 λ개 존재한다.

3.2 비밀분산방식의 행렬표현

s를 비밀, $v_1, v_2, \ldots, v_n$를 그 분산정보로 한다. Γ를 악세스집합의 족. 즉, 악세스구조로 한다. 비밀분산방식은 가능한 $(s, v_1, v_2, \ldots, v_n)$의 실현치를 행으로 하는 행렬에 의해 표현할 수 있다. 본 논문에서는 이와같은 행렬을 비밀분산행렬이라 하고 M으로 나타낸다. M을 이해하기 위해 예 1을 든다.

(예1) $n=3$, $\Gamma=\{\{v_1, v_2\}, \{v_2, v_3\}, \{v_1, v_2, v_3\}\}$의 비밀분산행렬 M은 이하와 같이 주어진다.

$$M=\begin{bmatrix} s & v_1 & v_2 & v_3 \\ 1 & 1 & 2 & 1 \\ 1 & 2 & 0 & 2 \\ 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \\ 2 & 2 & 1 & 2 \\ 2 & 0 & 2 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

분산정보의 분배자(Dealer)는 M의 행을 랜덤하게 선택하여 v_1, v_2, v_3의 값을 각각 멤버 1,2,,3에게 분배한다. v_1, v_2이 악세스 집합인 것은 예를 들면, $v_1, v_2=(1, 2)$일 때 $s=1$로서 유일하게 s가 결정되는 (M의 제 1행) 것으로부터 알 수 있다. 이에 반해 $v_1, v_3=(1, 1)$일 때는 $s=1$(제 1행) $s=2$ (제 4행) $s=0$ (제 7행) 과 s의 모든 값이 가능성을 갖는 즉, $v_1, v_3=(1, 1)$일 때는 s에 관한 정보를 알 수 없다. 이를 모든 (v_1, v_3)의 실현치에 대해 적용할 수 있으므로 $\{v_1, v_3\}$은 비악세스 집합임을 알 수 있다.

3.3 구성법

비밀분산방식의 악세스 구조가 갖는 행렬구조는 디자인구조가 갖는 행렬구조에 의해 표현될 수 있다. 본 절에서는 조합디자인이 갖는 행렬구조를 비밀분산행렬에 정합시키기 위해 각각 예를 들어 설명하고 구성법을 정리한다. 특정 조합디자인이 갖는 행렬구조를 비밀분산행렬로서 변환하고 이 비밀분산행렬이 갖는 비밀복원 특성을 추출하여 정리로서 요약한다.

(1) $OA_1(t, k, n)$에 근거한 비밀분산방식의 구성

(예 2) $OA_1(2, 4, 3)$의 구성

($OA_1(2, 4, 3)$은 (3, 2)임계치법의 비밀분산행렬 M이 되고 있다)

$$OA_1(2, 4, 3)=\begin{bmatrix} s & v_1 & v_2 & v_3 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 \\ 0 & 2 & 2 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 2 \\ 2 & 0 & 2 & 2 \\ 2 & 1 & 0 & 1 \\ 2 & 2 & 1 & 0 \end{bmatrix}$$

[정리1] $OA_1(t, k, n)$을 비밀분산방식의 비밀분산행렬이라고 한다. 이 행렬로부터 얻어지는 비밀분산방식은 $|s|=|v_i|=n$ 되는 $(k\text{-}1, t)$ 임계치법이다.

(증명) [정의 1]의 (2)로부터 이 비밀 분산행렬 M은 이하의 성질을 갖는다.

(i) s를 포함하지 않는 임의의 t열을 생각한다. 간단히 이것을 $(v_1, \ldots, v_t)$로 한다.
이 t열에 있어서 임의의 값 $(x_1, \ldots, x_t)$은 어느 한 행밖에 나타나지 않는다.
따라서 $v_1=x_1, \ldots, v_t=x_t$라는 값으로부터 이 행의 s값을 유일하게 결정할 수 있다.
그러므로 $(v_1, \ldots, v_t)$은 악세스 집합이다.

(ii) s를 포함하는 임의의 t열을 생각한다. 간단히, s이외의 t-1열을 $(v_1, \ldots, v_t)$로 한다.
이 t-1열의 임의의 값 $(x_1, \ldots, x_{t-1})$에 대해 s열의 값은 0으로부터 n-1까지가 1회 나타난다.
따라서 $(v_1, \ldots, v_{t-1})$는 비악세스 집합이다.
(i)(ii)로부터 이 비밀 분산방식은 (k-1, t) 임계치법이다.
$|s|=|v_i|=n$는 $OA_1(t, k, n)$의 정의로부터 명백하다.

(2) t-(v, k, 1) 디자인에 근거한 비밀분산방식의 구성

(예 3) 3-(10, 4, 1)디자인을 이하에 나타낸다.

$X=\{1, 2, \ldots, 10\}$
$D=\{1\ 5\ 6\ 7\}$
$\{1\ 2\ 8\ 9\}$
$\{2\ 3\ 7\ 10\}$
$\{3\ 4\ 6\ 9\}$
$\{4\ 5\ 8\ 10\}$
$\{2\ 3\ 4\ 8\}$
$\{3\ 4\ 5\ 7\}$
$\{1\ 4\ 5\ 9\}$
$\{1\ 2\ 5\ 10\}$
$\{1\ 2\ 3\ 6\}$
$\{1\ 3\ 5\ 8\}$
$\{1\ 2\ 4\ 7\}$
$\{2\ 3\ 5\ 9\}$
$\{1\ 3\ 4\ 10\}$
$\{2\ 4\ 5\ 6\}$

[정리 2] t-(v, k, 1) 디자인의 각 블록을 행으로 하는 행렬을 M으로 한다. 이 M을 비밀 분산행렬로 하는 비밀분산공유법에 있어서 임의의 t명은 악세스 집합이다.

(증명) [정의 2]의 (2)로부터 임의의 t열의 값 $(x_1, \ldots, x_t)$는 M의 행을 결정한다. 따라서 s를 포함하지 않는 임의의 t열의 값은 s열의 값을 유일하게 결정한다. 그러므로 임의의 t명은 악세스 집합이다.

(예 4) 예 3의 3-(10, 4, 1) 디지인으로부터 얻을 수 있는 비밀분산 행렬 M을 이하에 나타낸다.

$$M=\begin{array}{c} \begin{matrix} s & v_1 & v_2 & v_3 \end{matrix} \\ \begin{bmatrix} 1 & 5 & 6 & 7 \\ 1 & 2 & 8 & 9 \\ 2 & 3 & 7 & 10 \\ 3 & 4 & 6 & 9 \\ 4 & 5 & 8 & 10 \\ 2 & 3 & 4 & 8 \\ 3 & 4 & 5 & 7 \\ 1 & 4 & 5 & 9 \\ 1 & 2 & 5 & 10 \\ 1 & 2 & 3 & 6 \\ 1 & 3 & 5 & 8 \\ 1 & 2 & 4 & 7 \\ 2 & 3 & 5 & 9 \\ 1 & 3 & 4 & 10 \\ 2 & 4 & 5 & 6 \end{bmatrix} \end{array}$$

(3) GD디자인에 근거한 비밀분산방식의 구성

(예 5) GD(4, 1, 3; 12) 디자인을 나타낸다.
$X=\{1, 2, \cdots, 12\}$
$X_1=\{1, 2, 3\}$, $X_2=\{4, 5, 6\}$, $X_3=\{7, 8, 9\}$,

X_4= {10, 11, 12}
{1 4 7 10}
{1 5 8 11}
{1 6 9 12}
{2 5 9 11}
D= {2 6 7 12}
{2 4 8 10}
{3 6 8 12}
{3 4 9 10}
{3 5 7 11}

[정리 3] $GD(k, 1, n;v)$의 각 블록을 행으로 하는 행렬을 M으로 한다. 단 X_i에 포함되는 요소는 제 i열에 위치하도록 한다. (X_i는 [정의 3]에서 정의 된 것으로 한다.) 이 M을 비밀분산 행렬로 하는 비밀분산공유법에 있어서 임의의 2명은 악세스 집합이다. 또한, $|s|=|v_i|=n$

(증명) [정의 3]으로부터 $GD(k, 1, n;v)$는 2-(v, k, 1)디자인이다. 그러므로 [정리 2]로부터 임의의 2명은 악세스 집합이다. 또 [정의 3]의 (2-1) 및 M의 구성으로부터 $|s|=|v_i|=n$

(예 6) 예 5의 $GD(4, 1, 3;12)$디자인으로부터 얻을 수 있는 비밀 분산행렬 M을 이하에 나타낸다.

$$M=\begin{bmatrix} s & v_1 & v_2 & v_3 \\ 1 & 4 & 7 & 10 \\ 1 & 5 & 8 & 11 \\ 1 & 6 & 9 & 12 \\ 2 & 5 & 9 & 11 \\ 2 & 6 & 7 & 12 \\ 2 & 4 & 8 & 10 \\ 3 & 6 & 8 & 12 \\ 3 & 4 & 9 & 10 \\ 3 & 5 & 7 & 11 \end{bmatrix}$$

3.4 제안방식의 검토

우선, t-(v, k, 1)디자인등 조합디자인의 균형성 조건이 비밀복원 특성을 어느 정도 결정하는가를 검토한다. 비밀을 분산정보로 분할 부호화할 때 비밀복원 특성은 조합디자인 파라메터 t, k, λ에 의해 특징지워진다. 즉 분산정보를 점으로, 비밀분산함수를 블록으로 대응시키면 비밀복원 특성은 조합디자인 파라메터 t, k, λ에 있어서 k점중의 t개의 점이 주어지면 블록을 정확히 하나 결정할 수 있는 성질에 귀착된다. 조합디자인의 정의로부터 검토하면,

- 각 블록에 포함되는 점의 개수는 k이다(블록의 사이즈 k가 비밀을 복원할 수 있는 인원수에 대응하고 있다).
- t개의 서로 다른 점에 대해서 이들을 모두 포함하는 블록의 개수는 일정하다(t가 비밀을 복원할 수 있는 극소악세스 집합의 사이즈에 대응하고 있다).
- t개의 점을 포함하는 블록의 수는 λ이다(λ가 극소악세스 집합이 복원할 수 있는 비밀의 수에 대응하고 있다).

이와같이 멤버의 부분집합인 k명중에서 t명이 모여지면 비밀분산방식이 구성되고 극소악세스 집합인 t명은 λ=1개의 비밀 복원이 가능하다. 이와같은 관점으로부터 비밀분산 방식은 조합디자인 파라메터 t, k, λ에 의해 특징지울 수 있다. 이러한 파라메타를 사전에 지정해서 비밀분산방식을 구성하는 것이 조합디자인 접근법의 이점이다. 반면 기존의 비밀분산방식은 $GF(q)$상의 파라메타 q에 의존하고 있다.

본 논문은 조합디자인 관점으로부터 비밀복원 특성을 형식화함으로써 비밀분산방식을 다음과 같이 재정의한다.

[정의 4] 비밀분산방식은 다음과 같은 비밀복원특성을 만족하는 (P, F)이다. 여기서 P는 v개의 점(분산정보)의 집합, F는 사이즈 k의 P의 부분집합의 족에 대응 하는 비밀분산함수

의 집합이다.

1) k개의 점중 t개 이상의 점으로부터 비밀을 유일하게 결정할 수 있다.

2) k개의 점중 t-1개의 이하의 점으로부터는 비밀을 전혀 결정할 수 없다.

한편, [정리 1]은 n≠소수의 멱승에 대해서도 임계치법을 구성할 수 있는 가능성을 나타내고 있다. (Shamir의 방법은 n은 소수의 멱승에 한하고 있음)

또한 $OA_1(t, k, n)$은 $GD(k, 1, n;v)$, TD(k, l, n) (TD: Transversal Design) 및 차수 n의 서로 직교하는 k-2매의 라틴 방격(k-2 Mutually Orthogonal Latin Square of order n)과의 등가성이 알려져 있다[4][9]. 이러한 등가성으로부터 여러가지 조합디자인에 근거한 비밀분산방식의 구성이 가능하다. 즉 본 논문에서 제안된 3가지 방식은 파라메타를 매개로 서로 등가적인 성질을 갖고 있으며 어떤 한 방식으로부터 다른 방식의 구성이 가능하다는 것을 나타내고 있다.

4. 결 론

본 논문에서는 비밀분산방식의 악세스 구조를 조합디자인이 갖는 행렬구조의 관점에서 해석하는 것에 의해 비밀분산방식과 조합디자인이 밀접한 관계가 있음을 고찰하였다. 이러한 고찰을 통해 유한체 $GF(q)$상에서 선택가능한 비밀 사이즈를 더욱 융통성있게 선택할 수 있다. 또한 조합적 구조가 갖는 균형성등을 최대한 활용함으로써 키 분실등의 대책으로 비밀을 분산 보관하는 메카니즘을 설계할 경우 실현이 용이하다. 향후 과제로서는 본 논문에서 고찰된 구성법의 응용 연구가 검토되어야 할 것이며 복수의 비밀을 갖는 비밀분산방식과 조합디자인과의 관계에 대한 검토가 필요할 것이다.

참 고 문 헌

[1] Brickell E.F. and Davenport D.M : "On the classification of ideal secret sharing schemes.", J. Cryptology, 4, pp. 123-134(1991).

[2] Blundo C, De Santis A, Stinson D.R. and Vaccaro U.: "Graph decomposition and secret sharing schemes.", Eurocrypt'92, pp. 1-20(1992).

[3] Blundo C, De Santis A, Gargano L. and Vaccaro U.: "On the information rate of secret sharing schemes.", Crypto'90(1992).

[4] Beth T, Jungnickel D. and Lenz H.: "Design theory", Cambridge Univ. Press(1993).

[5] Benaloh J. and Letchter J.: " Generalized secret sharing and monotone functions", Advances in Cryptography-Proc. of Crypto'88, Notes Comp. Science, pp. 27-35 (1990).

[6] Blakley G. R: "Safeguarding Cryptographic keys", Proc, of AFIPS1979 Nat. Computer Conference 48, pp. 313-317 (1979)

[7] Asmuth C. A, Bloom J.: "A modulor approach to key safeguarding.", IEEE Tr. IT 29 pp. 208-210 (1983).

[8] Brickell E. F and Stinson D. R.: "Some improved bounds on the information rate of perfect secret sharing schemes", J. Cryptology (1991).

[9] Hughes D.R. and Piper F. C.: "Design theory", Cambridge Univ. Press, Cambidge (1985)

[10] Ito M., Saito A. and Nishizeki T.: "Secret sharing scheme realizing general access

structure", Proc. IEEE Globecom'87, pp. 99-102 (1987).

[11] Karnin E.D., Green J. W and Hellman M. E.: "On secret sharing systems", IEEE Trans, IT-29, 1, pp, 35-41 (1982)

[12] McEliece R.J, Sarwate D. : "On sharing secrets and Reed-Solomon codes", Comm ACM 24, pp583-584 (1981).

[13] Shamir A.: "How to share secret", Comm. of the ACM, 22, pp. 612-613 (1979)

[14] Stinson D. R : "New general lower bounds on the information rate of secret sharing schemes", Proc. of Crypto'92

□ 著者紹介

송 유 진

1978년 ~ 1982년 한국항공대학교, 학사
1985년 ~ 1987년 경북대학교, 석사
1992년 ~ 1995년 Tokyo Institute of Technology, 박사
1983년 ~ 1986년 공군기술장교
1988년 ~ 1996년 한국전자통신연구원 선임연구원
1996년 ~ 현재 동국대학교 정보산업학과 교수

※ 주관심 분야 : 암호이론, 정보이론, 컴퓨터통신, 전자상거래 보안 및 전자화폐