要 旨

秘密分散における効率的かつ高速な計算処理

嶋岡 哲夫

情報を安全に保管する方法のひとつとして秘密分散法があげられる．

過去の研究では，構成法に拡大体を用いて秘密分散法を実現した．この方法では，拡大体上の 2 項演算には演算表を用いているが，この演算表は膨大な容量を要する．

本研究では，拡大体の性質を考慮して四則演算は場合分けして行っている．加法については，直接 2 項演算と表引きするものとを場合分けしている．このとき用いる演算表は可換律を考慮して縮小を行っている．また，減法については，加法と演算結果が同じになるために考慮する必要がない．乗法および除法については，べき表現により直接 2 項演算している．これにより，乗法表と除法表を用いる必要がなくなった．

本研究の結果，実行の際の必要な容量を省き，拡大体上で効率よく秘密分散法を実行できる．

キーワード　秘密分散法，(k, n) しきい値法，拡大体，四則演算

Abstract

Fast Calculation for Secret Sharing Scheme

Tetsuo SHIMAOKA

The Secret Sharing Scheme(SSS) is a method to keep information out for safety.

In the past paper, The SSS is executed on the extension field $\boldsymbol{GF}(2^m)$.

On the extension field $\boldsymbol{GF}(2^m)$, it can't execute on two term calculation.

Then, it made operational tables for four operation rules solution of which can't execute on two term calculation. However, operational tables are large size, so they need enormous memory.

In this paper, two term calculation is distinguished character of the extension field $\boldsymbol{GF}(2^m)$.

Case of addtion, directly two term calculation and reference to operational table. then, this table is reduced by commutative law. Moreover, results of addtion and subtraction are equivalent, so subtraction doesn't need to consider.

Case of multiplication and division, it is possible exponential laws to calculate,so it doesn't need multi table and div table.

As a result,when SSS executes,it save extra memory.So,it is efficiency of SSS to executes on the extension field $\boldsymbol{GF}(2^m)$.

multiplication and division doesn't need to operational table, and addtion's table is less than half.

key words Secret Sharing Scheme(SSS), (k,n)threshold SSS, extension field, four operation rules