Secrect Sharing Progress

Joan Ngure

Report

Problem statement: In secret sharing schemes the shares must be of length at least as the secret itself (known fact). If the secret is short this known fact is efficient, else if it is long, this known fact is inefficient in terms of space and communication. For example if the secret is a large confidential file or a secret data base shared by several servers.
Problem questions: The known fact ensures perfect secrecy. What would happen if the secrecy is not perfect against resource bounded adversaries. Can shares be made significantly shorter to the secret size in this case?
Solution to the above question:

1. The resultant scheme achieves extreme space and communication efficiency. In an m-threshold scheme, m shares recover the secret but m-1 shares give no computation information about the secret. The size of the shares is $\frac{|S|}{m}$ plus a short piece of information whose length does not depend on the secret size but just in the security parameter. This bound $\frac{|S|}{m}$, is optimal if the secret is to be recovered by m shares.

2. The resultant solution combines the traditional secret sharing schemes with encryption and information dispersal techniques.

Robust scheme with the above properties (malicious participants cannot prevent the reconstruction of the secret by a legal coalition, even if the return modified shares. Of course this malicious participants must be bounded). This can be achieved by public key signatures or distributed fingerprints together with the above mentioned techniques.

Computation Secret Sharing:
In an m threshold scheme m-1 shares give no information about the secret S. Two notions of secrecy according to 'no information':

1. Perfect secrecy where no information is in the information theoretic sense.

2. Computation secrecy where no information can be efficiently computed.

The author goes ahead and gives notion of perfect indistinguishability.

secret sharing with short shares:
To achieve a space efficient secret sharing scheme, an information dispersal scheme with a secure encryption scheme and a perfect secret(eg shamir's) sharing scheme is combined.
information dispersal scheme is a scheme intended for the distribution of a piece of information among n active processors in an m threshold scheme. m active processors can recover the information assuming they are all honest. The idea is to add redundancy to a file F and partition it into n fragments, each transmitted to one party and the length of each fragment is $\frac{|F|}{m}$. This is clearly space optimal. This scheme can be implemented in varies ways, all corresponding to the notion of erasure codes in the theory of error correcting codes. The scheme does not deal with malicious parties or with the secrecy of information.

Robust secret sharing:
Assuming all parties are honest is a strong assumption. The robust secret sharing scheme can correctly recover in the presence of a bounded number of corrupted shares, while keeping the secret requirements. This scheme requires parties to submit their shares along with an unforgeable signature. Although this solution is space efficient, it requires implementation of a public key system to support public signatures. This comes at a cost with computation, administration and key management. In addition the dealer is required to be known plus a timestamp to prevent replay attacks. These drawbacks have been overcome with distributed fingerprints which requires no public key system, uses no secret keys at at all, does not require dealers identity or timestamp. It only requires majority of honesty parties and a global function of a one-way function.