Yale University
Department of Computer Science

Keeping Shares of a Secret Secret

Josh D. Cohen

YALEU/DCS/TR-453
February 1986

This work was supported in part by the National Security Agency under Grant MDA904-84-H-0004.

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
453

2. GOVT ACCESSION NO.

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
KEEPING SHARES OF A SECRET SECRET

5. TYPE OF REPORT & PERIOD COVERED
Technical Report

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
Josh D. Cohen

8. CONTRACT OR GRANT NUMBER(s)
NSA: MDA904-84-H-0004

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Department of Computer Science/ Yale University
Dunham Lab/ 10 Hillhouse Avenue
New Haven, CT 06520

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6000

12. REPORT DATE
February, 1986

13. NUMBER OF PAGES
11

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)

15. SECURITY CLASS. (of this report)
Unclassified

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Approved for public release; distributed unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Secret Sharing
Threshold Scheme
Homomorphism
Distributed Computing
Fault Tolerance
Protocol
Election
Voting

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

In 1979, Blackley and Shamir independently proposed schemes by which a secret can be divided into many shares which can be distributed to mutually suspicious agents. This report describes a homomorphism property attained by these and several other secret sharing schemes which allows multiple secrets to be combined by direct computation on shares. This property reduces the need for trust among agents and allows secret sharing to be applied to many new problems. One of these problems, that of secret-ballot elections, is given as an application.

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Keeping Shares of a Secret Secret

Josh D. Cohen

Abstract

In 1979, Blackley and Shamir independently proposed schemes by which a secret can be divided into many shares which can be distributed to mutually suspicious agents. This report describes a homomorphism property attained by these and several other secret sharing schemes which allows multiple secrets to be combined by direct computation on shares. This property reduces the need for trust among agents and allows secret sharing to be applied to many new problems. One of these problems, that of secret-ballot elections, is given as an application.

1 Introduction

Suppose that the economic ministers of the world are assembled in a room. They have agreed that a world economic forecast is desirable and that this cannot be accomplished without knowing the total assets of all the nations. Each minister knows the assets of his or her nation (a very closely guarded secret), and they all agree that it is in their common interest to determine their total assets so that the forecast can be completed. Being economists, however, the ministers are extremely skeptical of cryptographers, mathematicians, computer scientists, and other odd creatures. In particular, the ministers have no faith whatsoever that factoring is hard or that $\mathcal{P}$ is different from $\mathcal{NP}$ (they don't even believe that $\mathcal{P}$-TIME is different from $\mathcal{P}$-SPACE). The economists do, however, know a proof when they see it (they *do* believe that LOG-SPACE is different from $\mathcal{P}$-SPACE), but nothing is to be believed without a proof.

Can the ministers determine their combined assets without relying on unproven assumptions to protect their secret information?

This work was supported in part by the National Security Agency under Grant MDA904-84-H-0004.

Cryptographic solutions can be found by using a mix ([Cha81]) or the voting scheme of [DLM82] which essentially scramble the data so that the associations between the secrets and their owners are hidden. If this is not sufficient, techniques for computing with encrypted data (see [RAD78], [Yao82], [BlMe85], and [Fei85], for example) can be incorporated into these schemes so that the final result consists of only the aggregate value rather than a (disassociated) list of secrets. This approach to the problem, however, depends heavily upon cryptographic assumptions such as the difficulty of factoring.

In this paper, we shall consider an alternate approach to such problems in which no cryptography or cryptographic assumptions are required (although the data used may be encrypted for other reasons).

If there exists an agent which is trusted by all the ministers, then the problem has a simple solution. Each minister gives his or her information to the agent, and the agent computes and announces the total assets. However, if there is distrust, such a scheme is unacceptable. Even if the accuracy of the total is believed or can be verified, the agent knows all of the secret information, and can reveal any of it at will.

If, however, a group of n agents can be found such that each economic minister believes that at least k of the agents are dependable (in the sense that they are willing to cooperate faithfully) and that no more than $k-1$ of the agents are corrupt (in the sense that they would conspire to reveal any secrets they could derive), then a solution to this problem can be found by embedding the problem within a suitable secret sharing scheme.

Shamir's polynomial secret sharing scheme [Sha79] is ideal for this purpose. Each minister gives a share of his or her secret datum to each of the n agents. Each agent can then simply add its shares to form a single super-share. The properties of polynomial evaluation and interpolation and the details of Shamir's scheme ensure that the super-shares are themselves shares of the sum of the secrets. Thus, when the super-shares are revealed, the desired sum can be derived.

At this point, we assume that there are no attempts at subversion. The information is assumed to be correct, and the only concern is that some of the agents may surreptitiously collaborate in order to obtain secret information. In section 4, we shall see an example of how interactive proofs and cryptographic methods can be used to verify both the validity of the shares given to the agents and the accuracy of the composite results returned by the agents.

In general, suppose each of m parties holds a "sub-secret", and there exists a "super-secret" which is the composition of the sub-secrets under some known function (such as the sum or the product of the sub-secrets). The parties want to determine the super-secret without revealing their sub-secrets or depending upon cryptographic assumptions.

With an appropriate secret sharing homomorphism, shares of the sub-secrets can be distributed to the n agents such that any k can determine each of the sub-secrets. Each agent can then compose its "sub-shares" into a single "super-share" such that any k of the super-shares are sufficient to determine the super-secret.

The advantage of such a homomorphism is that k of the n agents can, by revealing their super-shares, determine the super-secret without sharing any information about the constituent sub-secrets. Information about the sub-secrets can only be obtained if k or more agents agree to merge their sub-shares to reconstruct the sub-secrets.

An application of this homomorphism will be seen in the domain of elections. Here a voter can distribute shares of his or her vote to n agents. Each agent can then compose its vote-shares to form a share of the election tally. If k or more of the agents reveal their composite tally-shares, then the election tally is publically revealed. However, a conspiracy of at least k dishonest agents is required in order to obtain information about an individual vote.

2 The Homomorphism Property

Shamir in [Sha79] defines a (k, n) *threshold scheme* to be a division of a secret D into n pieces $D_1, \ldots, D_n$ in such a way that:

1. knowledge of any k or more D_i pieces makes D easily computable;
2. knowledge of any $k-1$ or fewer D_i pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

Let S be the domain of possible secrets, and let T be the domain of legal shares. Every instance of a (k, n) threshold scheme determines a set of functions $F_I : T^k \rightarrow S$ defined for each $I \subseteq \{1, 2, \ldots, n\}$ with $|I| = k$. These functions define the value of the secret D given any set of k values $D_{i_1}, \ldots, D_{i_k}$:

$$D = F_I(D_{i_1}, \ldots, D_{i_k}),$$

where $I = \{i_1, \ldots, i_k\}$.

Let $\oplus$ and $\otimes$ be binary functions on elements of the secret domain S and of the share domain T, respectively. We say that a (k, n) threshold scheme has the $(\oplus, \otimes)$-*homomorphism* property (or is $(\oplus, \otimes)$-*homomorphic*) if for all I, whenever

$$D = F_I(D_{i_1}, \ldots, D_{i_k})$$

and

$$D' = F_I(D'_{i_1}, \ldots, D'_{i_k}),$$

then

$$D \oplus D' = F_I(D_{i_1} \otimes D'_{i_1}, \ldots, D_{i_k} \otimes D'_{i_k}).$$

This property implies that the composition of the shares are shares of the composition.

It is clear that Shamir's polynomial secret sharing scheme is $(+, +)$-homomorphic, but it is not quite so apparent that Shamir's scheme satisfies another property which is also necessary to capture the intuition described earlier.

We want it to also be the case that $k - 1$ sets of sub-shares together with all of the super-shares (and therefore the super-secret) leave the sub-secrets completely undetermined.

We define a $(\oplus, \otimes)$-*composite* (k, n) *threshold scheme* to be a division of a set of sub-secrets $d_1, \ldots, d_m$ into sub-shares $d_{i,j}, 1 \leq i \leq n, 1 \leq j \leq m$ such that

1. $D = d_1 \oplus d_2 \oplus \cdots \oplus d_m$ is easily computable given and k or more distinct super-shares $D_i = d_{i,1} \otimes d_{i,2} \otimes \cdots \otimes d_{i,m}$;
2. When $m > 1$, knowledge of D, all D_i, and any $k - 1$ or fewer sets of sub-shares $d_{i,1}, d_{i,2}, \ldots, d_{i,m}$ leave the sub-secrets d_j completely undetermined (in the sense that all its possible values are equally likely).

The following theorem is somewhat surprising,

Theorem 1 *If the secret domain S and the share domain T are finite and of the same cardinality, then every $(\oplus, \otimes)$-homomorphic (k, n) threshold scheme is a $(\oplus, \otimes)$-composite (k, n) threshold scheme.*

Proof: (sketch)

The definition of $(\oplus, \otimes)$-homomorphism implies condition (1) immediately.

To prove condition (2), it suffices to consider only the case when $m = 2$ (two sub-secrets). The case for arbitrary m follows easily by induction.

Let $\{F_I\}$ be the set of functions determined by the (k, n) threshold scheme, let $D = d_1 \oplus d_2$ be the (known) super-secret, and let $D_1, \ldots, D_n$ be the (known) super-shares. Assume without loss of generality that the sub-shares $d_{i,1}, d_{i,2}, \ldots, d_{i_k-1}$, for $i = 1, 2$, are known. We want to show that if $D = d_1 \oplus d_2 = d_1' \oplus d_2'$, then from the known information, each of (d_1, d_2) and (d_1', d_2') are equally likely to be the actual pair of sub-secrets.

Fix $I = \{1, 2, \ldots, k\}$ and consider F_I. By condition (2) of a (k, n) threshold scheme, and since $|S| = |T|$ (with finite cardinality), there exists exactly one value $d_{1,k} \in T$ such that $d_1 = F_I(d_{1,1}, d_{1,2}, \ldots, d_{1,k-1}, d_{1,k})$ and one $d'_{1,k} \in T$ such that $d_1' = F_I(d_{1,1}, d_{1,2}, \ldots, d_{1,k-1}, d'_{1,k})$. Similarly, there is exactly one value $d_{2,k} \in T$ such that $d_2 = F_I(d_{2,1}, d_{2,2}, \ldots, d_{2,k-1}, d_{2,k})$ and one $d'_{2,k} \in T$ such that $d_2' = F_I(d_{2,1}, d_{2,2}, \ldots, d_{2,k-1}, d'_{2,k})$. Also, there is exactly one possible value of $D_k \in T$ such that $D = F_I(D_1, D_2, \ldots, D_k)$.

If each of the pairs $(d_{1,k}, d_{2,k})$ and $(d'_{1,k}, d'_{2,k})$ can be shown to be equally likely, then the sub-secrets (d_1, d_2) and (d_1', d_2') that each would respectively imply also become equally likely. But this is true if both $d_{1,k} \otimes d_{2,k} = D_k$ and $d'_{1,k} \otimes d'_{2,k} = D_k$ are true.

We can see that this is the case from the following chains of equalities.

$$\begin{aligned}
D &= d_1 \oplus d_2 \\
&= F_I(d_{1,1}, d_{1,2}, \ldots, d_{1,k-1}, d_{1,k}) \oplus F_I(d_{2,1}, d_{2,2}, \ldots, d_{2,k-1}, d_{2,k}) \\
&= F_I(d_{1,1} \otimes d_{2,1}, d_{1,2} \otimes d_{2,2}, \ldots, d_{1,k-1} \otimes d_{2,k-1}, d_{1,k} \otimes d_{2,k}) \\
&= F_I(D_1, D_2, \ldots, D_{k-1}, d_{1,k} \otimes d_{2,k}).
\end{aligned}$$

Also,

$$\begin{aligned}
D &= d_1' \oplus d_2' \\
&= F_I(d_{1,1}, d_{1,2}, \ldots, d_{1,k-1}, d'_{1,k}) \oplus F_I(d_{2,1}, d_{2,2}, \ldots, d_{2,k-1}, d'_{2,k}) \\
&= F_I(d_{1,1} \otimes d_{2,1}, d_{1,2} \otimes d_{2,2}, \ldots, d_{1,k-1} \otimes d_{2,k-1}, d'_{1,k} \otimes d'_{2,k}) \\
&= F_I(D_1, D_2, \ldots, D_{k-1}, d'_{1,k} \otimes d'_{2,k}).
\end{aligned}$$

But we've seen above that the only possible value $* \in T$ such that

$$D = F_I(D_1, D_2, \ldots, D_{k-1}, *)$$

is D_k. Thus, both $d_{1,k} \otimes d_{2,k} = D_k$ and $d'_{1,k} \otimes d'_{2,k} = D_k$ are true, as desired.

Therefore, (d_1, d_2) and (d_1', d_2') are equiprobable values for the hidden pair of sub-secrets. ∎

It should be noted that in the above proof, the condition that the secret domain S and the share domain T are of the same finite cardinality was only used to assure that if D_k is a given super-share, then the probability that D_k was derived as some $d_{1,k} \otimes d_{2,k}$ which imply sub-secrets of d_1 and d_2, respectively is the same as the probability that D_k was derived as some $d'_{1,k} \otimes d'_{2,k}$ respectively implying sub-secrets of d'_1 and d'_2. This property may be attained by a secret sharing scheme even if the constraint on the domains is not.

3 Some Examples

It is easy to see that the properties of polynomials give Shamir's (k, n) threshold scheme the $(+, +)$-homomorphism property, and since the secret domain and the share domain consist of the same finite set (namely the integers modulo p), Shamir's scheme is a $(+, +)$-composite (k, n) threshold scheme and enjoys all of the properties thereof.

Some other techniques can also be easily seen to produce $(+, +)$-composite (k, n) threshold schemes. See [Bla79], [AsBl80], and [Kot84] for some further examples.

What if the super-secret is not the sum of the sub-secrets? By using a homomorphism between addition and discrete logarithms, it is possible to transform Shamir's scheme into a $(\times, +)$-composite (k, n) threshold scheme. Thus, if the desired super-secret is the product of the sub-secrets, Shamir's scheme can still be used.

In general, discrete logarithms may be difficult to compute. However, if p is small or of one of a variety of special forms, the problem is tractable (see [PoHe78], [Adl79], [CLS85]). It should be emphasized that such special cases for p do not in any way weaken the security of our schemes. The security is ***not*** cryptographic, but rather is information theoretic. Therefore, there need be no assumptions about the difficulty of solving any special problems.

4 Application: Secret-Ballot Elections

The motivating application for this work is in the domain of cryptographic elections. In [CoFi85], an election scheme is presented in which a government holds an election in which the legitimacy of the votes and the tally is verified by means of interactive proofs (see [FMR84], [GMR85]).

Although, there is high confidence in the correctness of the tally in such an election, the government is a "trusted authority" with the ability to see every vote and compromise the voters' privacy.

The election scheme can, however, be embedded within a $(+,+)$-composite (k,n) threshold scheme (in particular, in Shamir's scheme) as suggested by the outline below. This extension is also described in [Coh86].

Instead of a single government, n sub-governments (or *tellers*) each hold a sub-election. Each voter then chooses either 0 or 1 as a secret value (0 indicating a no vote, 1 indicating a yes vote) and distributes one share of the secret vote to each of the n tellers. The tally of the election will be the sum of the voters' secrets.

After votes are cast, each teller simply adds the vote-shares it has received. Since the (k,n) threshold scheme has the $(+,+)$-homomorphism property, this sum of vote-shares is itself a share of the sum (tally) of the votes. Thus, once k or more tellers release their sub-tallies, the overall election tally can be determined. Furthermore, since the secret domain and the share domain consist of the same finite set, the conditions of Theorem 1 are satisfied, and k or more conspiring tellers are required to determine any individual voter's secret vote.

Since each teller actually tallies the vote-shares it receives by means of the (single government) election scheme of [CoFi85], there is very high confidence that the sub-tally it releases is correct.

Also, the interactive proof techniques used in this scheme can be generalized slightly to allow verification of the vote-shares. Here, each voter participates in an interactive proof to demonstrate to all participants that the vote-shares it distributes are *legitimate* in the sense that every set of k vote-shares derives the same secret vote and that this vote is either a 0 or a 1.

Thus, as long as at least k of the n designated tellers participate through to conclusion, an election can be conducted such that each participant has very high confidence in the accuracy of the resulting tally and no set of $k-1$ or fewer tellers (together with any number of conspiring voters) can (without breaking the underlying cryptosystem and thereby solving an open number theoretic problem) gain more than a small ε advantage at distinguishing between possible votes of honest voters.