Safeguarding cryptographic keys

by G. R. BLAKLEY
Texas A&M University
College Station, Texas

INTRODUCTION

Certain cryptographic keys, such as a number which makes it possible to compute the secret decoding exponent in an RSA public key cryptosystem,[1,5] or the system master key and certain other keys in a DES cryptosystem,[3] are so important that they present a dilemma. If too many copies are distributed one might go astray. If too few copies are made they might all be destroyed.

A typical cryptosystem will have several volatile copies of an important key in protected memory locations where they will very probably evaporate if any tampering or probing occurs. Since an opponent may be content to disrupt the system by forcing the evaporation of all these copies it is useful to entrust one or more other nonvolatile copies to reliable individuals or secure locations. What must the nonvolatile copies of the keys, or nonvolatile pieces of information from which the keys are reconstructed, be guarded against? The answer is that there are at least three types of incidents:

- An *abnegation incident* is an event after which a nonvolatile piece of information is no longer completely reclaimable by the organization which entrusted it to a guard. There are three main types of abnegation incidents:
  —*Destruction* of the nonvolatile piece of information. For example, a person carrying a copy of a number can meet with an unexpected accident, during which the copy is destroyed.
  —*Degradation* of the nonvolatile piece of information. For example, a person may lose his copy of the number and, in embarrassment and confusion, produce some other number when asked.
  —*Defection* with the nonvolatile information. For example, the person with the copy of the number may divulge it to the opposition and refuse to tell it to the organization which entrusted it to him.
- A *betrayal incident* is an event after which a nonvolatile piece of information is completely known to an opponent of the organization which entrusted it to a guard. Defection, which we have already encountered among abnegation incidents, is one kind of betrayal incident. The other main kind of betrayal incident is
  —*Dereliction* with the nonvolatile piece of information, an act which reveals it to the opposition so as not to be discovered by the organization which entrusted it to the guard, either before or after he has been requested to return it. For example, the person who has the copy of the number can show it to an opponent but still play the part of a faithful guard, and even report the number back correctly when requested.
- A *combination incident* is an abnegation incident which is also a betrayal incident. The main kind of combination incident is defection. The three types of incident are, thus, A, B and C. And the commonest kinds of A, B or C incidents are the four Ds. Note that none of the four Ds need imply malfeasance, misfeasance or even nonfeasance on the part of the guard. But it would be wise to consider such possibilities whenever an incident of any of the three types is detected.

Why was simple loss of the nonvolatile piece of information not included above? The answer is that some types of loss amount essentially to destruction of the nonvolatile piece of information, in the sense that neither the organization that entrusted it to a guard nor any of its opponents is likely to get the piece of information before the encrypted information becomes valueless. For example, the person with the copy of the number was on a Mars flyby which lost contact forever with Earth as it went behind Mars. But if a loss cannot be confidently regarded as a destruction, the proverbial "prudent man," in charge of evaluating this incident for the organization which entrusted the nonvolatile piece of information to a guard, must regard it as a defection. For example, if the person who memorized the number disappeared after a family quarrel the prudent man evaluating the incident must assume that an opponent knows the piece of information in question.

COUNTING AND DISCOUNTING INCIDENTS

There are two principles for counting incidents. The first is Boole's law of inclusion and exclusion. Suppose that an organization issues nonvolatile pieces of information to guards and waits a modest period of time during which incidents occasionally occur. Let *a* stand for the number of abnegation incidents, *b* for the number of betrayal incidents and *c* for the number of combination incidents. The total number d of incidents is $d=a+b-c$ because a combination incident gets counted twice, once by a and once by b.

The second principle is that incidents are so rare, that the possibility of two separate incidents occurring with the same nonvolatile piece of information is usually dismissed on probabilistic grounds as absurd. A defection is a single incident with two aspects, abnegation and betrayal, so it is not dismissed as too improbable. But the idea that the person who has a copy of the number dies in a plane crash one month after confiding it to an opponent *is* dismissed as too improbable. Too slavish an adherence to this "second-order improbability" prejudice can lead to ludicrously inappropriate actions, such as that of the statistician who always carries his own bomb on airplanes because it is so improbable that there will be two bombs on the same flight. But it is a good rule of thumb if used properly.

This latter principle implies, among other things, that none of the four numbers a, b, c or $a+b-c$ exceeds the number g of nonvolatile pieces of information entrusted to the g guards.

Suppose an organization chooses in advance the number a of abnegation incidents and the number b of betrayal incidents it feels it must be protected against when entrusting several nonvolatile pieces of key reconstruction information to a set of guards. Each guard gets a different piece of information. The lifetime of this scheme must not be very many months if separate incidents involving the same piece of information are to be ruled out. We know that $c \leq MIN\{a,b\}$ since a combination incident is both an abnegation incident and a betrayal incident. From the two counting principles above it then follows that

$$a+b-MIN\{a,b\} \leq d \leq a+b$$

and that $d \leq g$, where g is the number of guards to which the organization entrusts the g nonvolatile pieces of information.

The prudent man, when designing a system of safeguarding key information which is secure from a abnegation incidents as well as b betrayal incidents, must assume that the number c of combination incidents is zero. This means that the maximum number of incidents must be anticipated, since

$$d=a+b-c=a+b-0$$

in this case. Such a key information safeguarding system must have the property that $a+b+1$ different nonvolatile pieces of key reconstruction information are generated, and given to distinct guards. The key must be reconstructible from any $b+1$ of these pieces (this assumes a abnegation incidents) but there must be no information whatever about the key which can be inferred from knowledge of only b of these pieces (this is protection against b betrayal incidents). This last requirement is unusual. For example, a polynomial of degree b can be reconstructed from its values at $b+1$ points. But already its values at any b points tell a lot about it. It can also be reconstructed from the values of its 0th through bth Taylor coefficients at a point. But already the values of any b of these $b+1$ numbers tell a lot about it. What we are asking for, then, is somewhat couunter-intuitive. Let us a coin a metaphor to describe it. We want to give every one of $a+b+1$ guards a shadow of a different profile of the key, so that the key can be reconstituted in its entirety from any $b+1$ of these shadows. However, somebody who has seen only b such shadows should be completely in the dark, in the very strong sense that any key on the keyring could cast these b shadows when illuminated from b appropriately chosen directions.

Let us look at what happens if $a=b=4$. Then any five of the nine guards have the wherewithal to reconstruct the key. Thus, there is considerable protection against defection and dereliction, since even four of the nine pieces of information are not enough to reveal anything at all about the key to an opponent. There is also protection against destruction. If the four pieces of information belonging to any four guards are destroyed the other five can still be used to reconstruct the key. As to degradation, suppose that six guards give correct reports of the shadows they carry, to return to the metaphor. Then there are six different sets of five guards whose pieces of information can reconstitute the same key. If the other three misreport their shadows then any one of the 120 sets of five guards containing at least one of the misreporting three guards will give a description of the key, but probably all these descriptions will differ among themselves and will also differ from the true value of the key. Thus, the six reports of different sets of five guards which agree are singled out as correct. Of course, if it is possible to tell whether a proffered key is the right one, then it is possible to reconstruct the key when only five guards report correctly. So protection against degradation need not be synonymous with protection against destruction, but they are largely concomitant with each other. In the approach to be discussed it will be assumed that the right key can be recognized when proffered. This assumption is reasonable since lists of plaintext to cryptext pairs can be publicized for testing as a backstop to the simpler test, which is that stored ciphertext messages will probably yield nonsensical diecipherments under a false key.

The rest of the paper describes one way to cast the $a+b+1$ shadows of a key in such a fashion that it can be reconstructed from any $b+1$ of them, but that no b of them tell anything about it whatever. The way this is done is to set up a many-to-many correspondence between keys and one-dimensional vector subspaces of (i.e. lines through the origin of) a finite vector space, F. One key determines a vast collection of lines but one line determines a tiny collection of keys. When an organization has a key to apportion among $a+b+1$ guards, it picks at random one of the lines corresponding to that key. Let us call this line L. Then it picks at random $a+b+1$ vector subspaces of f—the shadows of the key—such that any b or fewer of them intersect in a large vector subspace of F whose various one dimensional vector subspaces lead back to all possible keys with approximately equal probability, but such that any $b+1$ of them intersect in L. Once L has been found there are only a few possible keys which could have given rise to it. Each one is tried against a stored list of plaintext to cryptext pairs and the correct one identified. This is not the first application of projective geometric ideas to problems involving codes.[2]

SOME PRELIMINARY RESULTS

$a \uparrow b$ is the bth power of a, and $a*b$ is the product of a and b.

- *Lemma* 1—Let a and b be positive integers. Let R be a set with at least $a+b+2$ members. Then there are more than $a+b+2$ subsets of R which consist of $b+1$ objects. There are more than $a+b+1$ subsets of R which consist of b objects. If f and g are two members of R there are more than $a+b$ subsets of $R\setminus\{f\}$ which consist of b objects, and there are at least $a+b$ subsets of $R\setminus\{f,g\}$ which consist of b objects.
- *Lemma* 2—Suppose that a and b are positive integers smaller than z. Let M be a matrix with at most $a+b+2$ rows and at most $b+2$ columns. Then M has as most $(z+1)(2z)$ entries and at most $(z+1)\binom{2z}{z}$ $b+1$ by $b+1$ submatrices. Thus M has fewer than $3z \uparrow 2$ entries and fewer than $4 \uparrow z$ submatrices of size $b+1=\text{by}=b+1$.
- *Lemma* 3—Suppose that $0<2Ex<2Q<2<E$. Then $2|(1-x) \uparrow E-(1-Ex)|<Q \uparrow 2$.
- *Lemma* 4—If $4 \leq A<B$ then $\Pi(1-j/B)<\Pi(1-2/B)$, where the products are over positive integers $j<A$.
- *Lemma* 5—Suppose that A and B are integers and that

$$0<2(A-1) \uparrow 2<2BQ<2B<(A-1)B.$$

Then $1-2Q<B!/([(B-A)!]*[B \uparrow A])<1$, and $1-2Q<((B-2)/B) \uparrow A<((B-1)/B) \uparrow A<1$.

- *Lemma* 6—Suppose that A and B are integers and that

$$0<2(A-1) \uparrow 2<2BQ<2B<(A-1)B$$

Suppose that a sample of A points (with replacement) is taken from a population of B points. Then the probability U that all sample points are distinct exceeds $1-2Q$. If two distinguished points of the population are specified in advance the probability V that no sample point is equal to either of them exceeds $1-2Q$. Therefore it follows *a fortiori* that if one or two distinguished population points are specified in advance, then the probability W that none of the points of the sample is equal to any of the distinguished points or to any other point of the sample exceeds $1-4Q$.

•*Lemma* 7—Let p be an odd prime. Let d be a positive integer. Let $S(d,p)$ be the collection of all d by d matrices with entries taken from the field F of integers modulo p. Let v and w be two non-zero members of F. Then there are as many members of $S(d,p)$ with determinant equal to v as there are with determinant equal to w.

•*Lemma* 8—Let p be an odd prime. Let k and n be positive integers. Let $f(p,n,k)$ be the number of k by n matrices over the field F of residue classes *modulo* p whose rank is less than k. Then $f(p, n, 1)=1$ and, whenever $2 \leq k \leq n$,

$$f(p, n, k)=p \uparrow [(k-1)(n+1)]+(p \uparrow n-p \uparrow (k-1))\ f(p, n, k-1).$$

Consequently,

$$p \uparrow [(k-1)(n+1)]<f(p, n, k)<p \uparrow [(k-1)(n+2)]+(p \uparrow n)\ f(p, n, k-1)$$

for every integer k such that $2 \leq k \leq n$.

•*Lemma* 9—Let p be an odd prime. Let $f(p, n, k)$ be as in Lemma 8. Then $p \uparrow (n \uparrow 2-1)<f(p, n, n)<2p \uparrow (n \uparrow 2-1)$.

- Theorem 1—Let p be a prime larger than 6. Let d be a positive integer. Let $S(d,p)$ be the collection of all d by d matrices with entries taken from the field F of integers *modulo* p. If $v \in F$ let $n(v, d, p)$ be the number of members of $S(d,p)$ whose determinant is equal to v. Suppose that h and g are members of F. Then

$$n(h, d, p)<3n(g, d, p)$$

and $[p \uparrow (n \uparrow 2-1)]/2<f(p,n,n)<2p(n \uparrow 2-1)$.

Thus, all determinants occur approximately equally often. In fact every non-zero field element occurs equally often as the value of the determinant of a member of $S(d,p)$ but zero occurs more often, though not thrice as often.

- *Theorem* 2—Let a, b and p be positive integers. Let M be a matrix with $a+b+2$ rows and $b+2$ columns. Suppose that

$$0<2[(a+b+2)(b+1)-1] \uparrow 2<2pQ<2p <[(a+b+2)(b+1)-1]p.$$

Suppose that one position in each row of M is chosen at random, and that that entry is set equal to 1. Suppose that the remaining $(a+b+2)(b+1)$ entries of M are chosen at random (with replacement) from the population of all p residue classes *modulo* p. Then each of the two events

1. Two entries of M, neither of which is one of the $a+b+2$ entries which were set equal to 1 at the outset, are congruent to each other *modulo* p
2. An entry of M, other than one of the $a+b+2$ entries which were set equal to 1 at the outset, is congruent to either 0 or 1 *modulo* p

have probability smaller than $2Q$. Consequently, the probability that neither Event 1 nor Event 2 occurs exceeds $1-4Q$.

It is easy to verify that if $Q=1/10 \uparrow 7$, and a and b are both smaller than 10, then it suffices to choose any $p>10 \uparrow 12$ in order to satisfy the hypotheses of Theorem 2. This is the order in which users of the keyguard system will usually proceed. The tiny positive number Q is a measure of the departure from complete randomness of the concealing procedure. The modest-sized positive integer a (resp. b) is the number of abnegation (resp. betrayal) incidents to be guarded against. After deciding on these three safety levels a user must then accept a value of p as large as dictated by the hypotheses of Theorem 2 in order to achieve them. The keyspace will then be chosen to contain at least p keys.

Consider, now, the probabilistic interpretation of Theorem 1. If you choose a member x of the field F of integers *modulo p,* and choose some d by d matrix M over F at random (by choosing its successive entries at random with replacement from f) then the probability W that $det(M)=x$ satisfies the inequality $1/2p<W<2/p$.

We will assume that the manner in which the matrix in

Theorem 2 is chosen (salting each row with a 1 entry) does not do much violence to this conclusion. In other words, we will make the following (unproven but plausible) assumption.

- *Hypothesis* 1—Let p be an odd prime. Let a and b be positive integers. Let M be a matrix with $a+b+2$ rows and $b+2$ columns. Suppose that a position in each row is chosen at random and that that entry is set equal to 1. Suppose that, thereafter, each of the remaining $(a+b+2)(b+1)$ entries is chosen at random from the field F of residue classes *modulo* p. Suppose that, then, a collection of $b+1$ row indices is chosen at random from the set of all $b+1$ member subsets of the set of all $a+b+2$ row indices. Suppose, finally, that a collection of $b+1$ column indices is chosen at random from the set of all $b+1$ member subsets of the set of all $b+2$ column indices. Let x be a member of F. Let W be the probability that the value of the determinant of the $b+1$ by $b+1$ submatrix S of M corresponding to these row and column indices is equal to x. Then W satisfies the inequality

$$1/2p < W < 2/p.$$

To put matters in a nutshell, a judicious salting of an otherwise randomly chosen matrix with a few entries equal to 1 should not cause the determinants of its large square submatrices to depart from the quite uniform distribution that determinants of completely randomly selected matrices exhibit.

GUARDING KEYS

A key k is a positive integer. A keyset K is a finite set of keys. Let B be the largest member of the keyset K. A reasonably small positive integer z is chosen. On practical grounds z should probably be smaller than 100. Two positive integers a and b smaller than z are chosen. A prime p only slightly smaller than B is found. It would not, in fact, be too expensive to find the largest *pseudoprime* smaller than B and let it be p. A pseudoprime is a large positive integer which satisfies a considerable number of Rabin's (hopefully) stochastically independent necessary[4] conditions for primality, and can therefore be assumed to be prime with a probability in excess of 0.99999 99999 99999 99999, or even more, if desired. Though p might be composite we shall regard it as prime in the development below. Let F be the field of integers *modulo* p. Let V be the $b+2$ dimensional vector space over F which consists of all lists (written in the form of rows) of $b+2$ members of F. For every member g of the set G of $a+b+1$ guards we will define a corresponding $b+1$ dimensional vector subspace $V(g)$ of the $b+2$ dimensional vector space V. To each key k there will correspond many lines, through the origin of V, representing k. The organization wishing to entrust k to a set of guards will choose one of these lines at random and call it $L(k)$. When b guards intersect their subspaces the intersection must be at least two-dimensional. Moreover, it will be such that its various one-dimensional vector subspaces represent all members of F with approximately equal likelihood. But when $b+1$ guards intersect their subspaces the intersection is the line $L(k)$, which does not depend on which $b+1$ guards were chosen. To $L(k)$ there will correspond only $b+2$ possible keys. The candidates can be checked and the key reclaimed. The rest of this section fleshes out this outline.

To begin we pick z and choose positive integers a and b smaller than z. Then we choose a small Q, and thereafter a suitably large p to satisfy the inequalities in the hypotheses of Theorem 2. We construct a matrix M with $a+b+2$ rows and $b+2$ columns as follows. For each row of M we pick an entry at random and set it equal to 1. Next we pick an entry at random in the first row of M and choose its value k at random from F. Then we choose the remaining $(a+b+2)*(b+2)-1$ entries of M at random (with replacement) from F. Now we test M for acceptance or rejection. In order to pass the first test M must have only one 1 in each row, it must have no zero entry and no two of its entries can be equal unless they are both equal to 1. Since a and b are non-negative integers smaller than z it follows from Lemma 2 that there are fewer than $3z \uparrow 2$ entries of M. Since p and Q satisfy the inequalities in the hypotheses of Theorem 2, it then follows from Lemma 4 that such a random process will produce a matrix which passes the first test with probability in excess of $1-2Q$. In order to pass the second test M must have no $b+1$ by $b+1$ submatrix whose determinant, calculated in F, is zero, and must have no two $b+1$ by $b+1$ submatrices whose determinants, calculated in F, are equal. There are fewer than $4 \uparrow z$ such submatrices, according to Lemma 2. The foregoing suggests that the random process which produced M will cause it to pass the second test with probability in excess of $1-2Q$. Therefore, it should pass both tests with probability in excess of $1-4Q$. In other words, the process used almost always produces a usable matrix M the first time it is employed. Once a matrix M passes the tests we know from Lemma 1 that we can form more than $a+b+1$ sets of $b+1$ rows of M which contain the first row of M. So we pick $a+b+1$ different sets of $b+1$ rows of M, each of which contains the first row of M. Each such set is linearly independent since every $b+1$ by $b+1$ submatrix of M is non-singular. Let $N(j)$ be the $b+1$ by $b+2$ submatrix of M formed in the obvious way from the jth of these $a+b+1$ sets of rows. Its first row consists of the first of M's rows which occurs in the set. Its second row is M's second. And so on. Now for each $x \in V$ it is possible to form the $b+2$ by $b+2$ matrix $Y(j,x)$ from $N(j)$ by appending a last (i.e. $(b+2)$nd) row

$$\begin{aligned} x &= (x(1), x(2), \ldots, x(b+1), x(b+2)) \\ &= (Y(j,x)[b+2,1], Y(j,x)[b+2,2], \ldots, \\ &\quad Y(j,x)[b+2,b+1], Y(j,x)[b+2,b+2]) \end{aligned}$$

The $b+1$ dimensional vector subspace of the vector space of rows with $b+2$ entries taken from F determined by $N(j)$ is the set

$$U(j) = \{x | det(Y(j,x)) = 0\}$$

Evidently the first row f of M belongs to $U(j)$ for every j since $Y(j,f)$ has first and last row equal to f for every j.

So when $b+1$ of these $b+1$ dimensional vector subspaces of the $b+2$ dimensional vector space of rows of $b+2$ entries taken from F are intersected their intersection is the line through the origin which also contains the vector f which is the first row of M. The equation $det(Y(j,x))=0$ is, of course, a linear equation of the form

$$c(j,1)x(1)+c(j,2)x(2)\ .\ .\ .\ +c(j,b+1)$$
$$x(b+1)+c(j,b+2)x(b+2)=0$$

where $c(j,t)$ is a determinant of some $b+1$ by $b+1$ submatrix of M. These are non-zero, and pair-wise unequal by the way M was produced. And, because of the foregoing, they probably appear to be approximately randomly selected from F.

But now look at what happens when only b of these subspaces is intersected to form a two-dimensional vector subspace. This means choosing integers

$$1\leq j(1)\leq j(2)<\ .\ .\ .\ <j(b)\leq a+b+1$$

and solving the simultaneous equations

$$\begin{gathered} det(Y(j(1),x)=0 \\ det(Y(j(2),x)=0 \\ \vdots \\ det(Y(j(b),x)=0 \end{gathered}$$

for x, by using Gauss elimination, then choosing a basis of two vectors for this space of all such x. The two-dimensional vector space in question contains the first row of M. But the randomness of the choices of the members of M should mean the following:

- *Hypothesis* 2—Consider the collection of all vectors in this two dimensional subspace which have exactly one entry equal to 1 and which have pairwise distinct entries none of which is zero. Any two members of $F\setminus\{0,1\}$ will be represented approximately equally often in the count of multiplicities of occurrence of members of $F\setminus\{0,1\}$ as entries in the vectors of this collection.

If this is correct then isolation of this two-dimensional subspace sheds no light whatever on how to recover the key. The recovery system, when you have $b+1$ subspaces $U(j)$ is to solve the system

$$\begin{gathered} det(Y(j(1),x))=0 \\ \vdots \\ det(Y(j(b+1),x))=0 \end{gathered}$$

as above. The solution is a line through the origin. A basis for it is a single vector $g=(g(1),g(2),\ .\ .\ .,\ g(b+1,g(b+2))$ which is some non-zero multiple of f, the first row of M, which contains the key as one of its entries. You know g, not f. But for each entry $g(i)$ of g it is easy to find the $h(i)\in F$ such that $g(i)h(i)\equiv 1\ mod(p)$. The $b+2$ vectors

$$\begin{gathered} h(1)g \\ h(2)g \\ \vdots \\ h(b+2)g \end{gathered}$$

are the only multiples of g which have 1 as an entry. Therefore f is among them, and the key k is among the entries of f. So one of the $(b+2)\uparrow 2$ entries on the list of vectors above is the key. And the key is not equal to 1, which occurs once among the entries of each vector. So there are

$$(b+1)(b+2)\leq z(z+1)$$

candidates to be tested. One of them will pass the test.

REFERENCES

1. Blakley, G. R., and I. Borosh, "Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages," *Computers and Mathematics with Applications*, Vol. 5, 1979 (in press).
2. Gilbert, E. N., F. J. MacWilliams and N. J. A. Sloane, "Codes which detect deception," *The Bell System Technical Journal*, Vol. 53, 1974, pp. 405-424.
3. Morris, R., N. J. A. Sloane and A. D. Wyner, "Assessment of the National Bureau of Standards proposed federal Data Encryption Standard," *Cryptologia*, Vol. 1, 1974, pp. 281-306.
4. M. Rabin, "Probabilistic algorithms," in *Algorithms and Complexity* J. Traub (ed.), Academic Press, 1976.
5. Rivest, R. L., A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, Vol. 21, 1978, pp. 120-126.