KEY MINIMAL AUTHENTICATION SYSTEMS FOR UNCONDITIONAL SECRECY

Philippe Godlewski(*) Chris Mitchell(**)

Abstract

This paper is concerned with cryptosystems offering unconditional secrecy. For those perfect secrecy systems which involve using key just once, the theory is well established since Shannon's works ; however, this is not the case for those systems which involve using a key several times. This paper intends to take a rigorous approach to the definition of such systems. We use the basic model for a security code developped by Simmons, initially for unconditional authentication. We consider the definition of perfect L-fold secrecy given by Stinson and used by De Soete and others. We consider other definitions : Ordered Perfect L-fold secrety and Massey's Perfect L-fold secrecy, and attempt to classify them. Lower bounds are given for the number of keys in such perfect systems, and characterisation of systems meeting these lower bounds are obtained. The last part of the paper is concerned with discussing examples of key minimal systems providing unconditional secrecy.

1. SCOPE AND PURPOSE

Two of the main applications of cryptography are the provision of secrecy and/or authentication for messages. In 1949 Shannon, [Shan1], showed how to construct systems offering unconditional secrecy, i.e. theoretically perfect secrecy systems, at the expense of the use of very large key spaces. Following this work on secrecy, Simmons, [Simm1], and others, [Bric1], [Gilb1], have considered systems which offer unconditional authentication, again at the expense of requiring very large numbers of keys.

In fact, most practical security systems are not theoretically secure, and could be broken given unlimited computational resources. Such practical security systems are based on reasonable assumptions about the difficulty of certain computational problems, and have the advantage of using manageable numbers of keys.

Nevertheless, unconditionally secure systems do find a use in certain special applications, e.g. the Washington-Moscow 'Hot Line', [Mass1]. It is also interesting to note that, although such 'perfectly secure' systems have been studied for nearly 40 years, the theory is not fully developed, at least in the public domain. It is the purpose of this paper to contribute to the development of this theory.

In particular, it attempts to classify a number of different definitions of perfect secrecy. Developing from this discussion of definitions, lower bounds are given for the number of keys in such perfect systems, and theorems characterising systems meeting these lower bounds ('key-minimal systems') are obtained. The last part of the paper is concerned with discussing examples of key-minimal systems providing unconditional secrecy.

2. NOTATION

We use the basic model for a security code developed by Simmons, [Simm1], and used by Brickell, [Bric1], De Soete, [DeSo1], [DeSo2] and Stinson, [Stin1], [Stin2].

(*) Département réseaux, Télécom Paris, 46 rue Barrault
75634 Paris cedex 13 France
(**) Hewlett-Packard Ltd. Filton Road, Stoke Gifford,
Bristol BS12 6QZ, England.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 497-501, 1990.

In this model there are three parties: the transmitter, T, the receiver, R, and an opponent, O. The transmitteT wishes to send R one or more pieces of information $s \in S$ in such a way that they cannot be read (secrecy) and/or modified/impersonated (authentication) by O. Users T and R achieve this by using a secret, pre-agreed encoding rule $e \in E$; this encoding rule e may be regarded as the cryptographic transformation corresponding to a secret key. It is always assumed that O knows the system (i.e. the Security Code) completely, the only secret is the encoding rule (i.e. the key) in use. Then T emits $m = e(s)$ which is actually transmitted and, perhaps, intercepted by O. The objective is to design a scheme which protects T and R from O.

More formally, a Security Code consists of three sets: a set S of *Source States*, a set M of encoded messages and a set E of encoding rules. Each encoding rule e is an injective function from S into M (we do not allow *splitting* here). We write k for $|S|$, v for $|M|$ and b for $|E|$ throughout, and, following De Soete, [DeSo1], [DeSo2], write SC(k,v,b) for a Security Code with k source states, v encoded messages and b encoding rules.

We consider various probabilities. We write $p_S(s)$, $p_E(e)$, and $p_M(m)$ for the a priori probabilities of occurrence of source state, encoding rule and message. We suppose $p_S(s)>0$ and $p_E(e)>0$ for every $s \in S$, and $e \in E$.. We write $p_{S|M}(s|m)$, $p_{M|S}(m|s)$, $p_{S|E}(s|e)$, ... for the conditional probabilities. We also abuse this notation slightly by writing $p_S(\underline{s})$ for L-tuple (or ordered set) $\underline{s} = (s_1, s_2, ...s_L)$ or $p_S(S')$ for L-set (unordered) $S' = \{s_1, s_2, ...s_L\}$ in S. We assume that encoding rule e and the different source states $s_1, s_2, ...s_L$ are chosen independently.

A set M' of messages is **allowable** if $p_M(M')>0$. In other words, M' is allowable iff M' could correspond to a set of messages encoded under a single encoding rule.

3. DEFINITIONS OF 'PERFECT' SECRECY

The initial problem that needs to be overcome in a formal study of cryptosystems providing unconditional or 'perfect' secrecy is the fact that existing definitions vary. Therefore, before attempting to study such systems we review the existing definitions, and indicate the relationships between them.

The first definition we give is a slightly modified version of a definition due to Stinson, [Stin1], [Stin2].

Given $L \geq 1$, an SC(k,v,b) is said to provide **Unordered Perfect L-fold secrecy (U(L)-secrecy)** if for every allowable L-subset M' of M and for every L-subset S' of S:
$p_{S|M}(S'|M') = p_S(S')$.

The second definition we give is the unmodified form of Stinson's definition, [Stin1], [Stin2].

Given $L \geq 1$, an SC(k,v,b) is said to provide **Stinson Perfect L-fold secrecy (S(L)-secrecy)** if for every allowable L'-subset M' of M and for every L"-subset S' of S ($L" \leq L' \leq L$) :
$p_{S|M}(S'|M') = p_S(S')$.

The following lemma is immediate from the definitions:

Lemma 3.1 An SC(k,v,b) provides S(L)-secrecy if and only if it provides U(L')-secrecy for every L' satisfying $1 \leq L' \leq L$.

However U(L)-secrecy by itself is not sufficient to guarantee S(L)-secrecy. For example, any SC(k,v,b) provides U(k)-secrecy, but will not necessarily provide S(k)-secrecy. Note that both these definitions are concerned with unordered sets of messages. A scheme providing

S(L)-secrecy protects its users against the opponent O gaining any information about the content of a set of L intercepted messages. However, such a scheme will not necessarily prevent O gaining information about the possible orderings of source states corresponding to observed messages. To provide this stronger notion of secrecy requires the use of a scheme satisfying our third definition, as follows:

Given L≥1, an SC(k,v,b) is said to provide **Ordered Perfect L-fold secrecy (O(L)-secrecy)** if for every allowable L-tuple $\underline{m}$ of distinct messages from M and for every L-tuple $\underline{s}$ of distinct source states from S : $p_{S|M}(\underline{s}|\underline{m}) = p_S(\underline{s})$.

It is then straightforward to establish:

Lemma 3.2 If an SC(k,v,b) provides O(L)-secrecy then it also provides O(L')-secrecy for every L' satisfying $1 \le L' \le L$.
We also have:

Lemma 3.3 If an SC(k,v,b) provides O(L)-secrecy then it also provides S(L)-secrecy.

Before proceeding to our fourth (and final) definition it is important to note that all the above definitions relate to 'ciphertext-only' attacks. Essentially, they are all concerned with the situation where the opponent O has intercepted L encoded messages and wishes to deduce information about the corresponding set of L source states. We now consider a definition of perfect security (due to Massey, [Mass1]) based on the concept of a 'known plaintext' attack.

Massey defines a known plaintext attack of order i to be an attack where the opponent O has intercepted i valid and distinct plaintext/ciphertext pairs (i.e. source state/encoded message pairs) all encrypted using the same encoding rule, e say. O is also assumed to have a further encoded message, produced using e and distinct from the messages in the i pairs, for which he wishes to obtain information about the corresponding source state. Then the attack will be said to 'succeed' if, for any source state s distinct from the states in the i pairs, the probability that s corresponds to m given the knowledge of the i pairs is different from the a priori probability of s (given that it is known that it differs from the source states contained in the i pairs).

An SC(k,v,b) is said to provide **Massey Perfect L-fold secrecy (M(L)-secrecy)** if, for any $i < L$, the scheme is secure against an order i known plaintext attack.

Note that the above definition is intended to be precisely the same as Massey's except that what we call M(L)-secrecy is what Massey calls Perfect (L-1)-fold secrecy. We have modified the definition so that it corresponds more closely with the other definitions given here. An equivalent definition of M(L)-secrecy, and one that fits more naturally with the other definitions is as follows:

Consider any SC(k,v,b). Let $\underline{s}$ be any i-tuple of distinct source states and let $\underline{s}'$ be the unique (i-1)-tuple derived from $\underline{s}$ by deleting its last entry. Let $\underline{m}$ be any allowable i-tuple compatible with $\underline{s}'$ for some encoding rule $e \in E$. Then, the SC(k,v,b) provides M(L)-secrecy if and only if for every $i \le L$, and for every $\underline{s}$, $\underline{s}'$, $\underline{m}$ as above :
$p(\underline{s}|\underline{m},\underline{s}') = p(\underline{s}|\underline{s}')$.

It is perhaps surprising to discover that Massey's definition is no stronger than the previous one. In fact we have:

Theorem 3.4 If an SC(k,v,b) provides O(L)-secrecy then it also provides M(L)-secrecy.

From now on, although it may be a little more powerful, we use the definition of O(L)-secrecy rather than that of M(L)-secrecy, since it appears to be easier to handle. Before proceeding note also that, for L = 1, all the above definitions coincide and in fact equate to Shannon's notion of perfect secrecy, [Shan1].

4. BOUNDS FOR L-SECURE SYSTEMS

We now consider a variety of bounds which can be established for L-secure systems of various types. We start by considering the weakest form of L-secrecy, namely U(L)-secrecy.

Lemma 4.1 If an SC(k,v,b) provides U(L)-secrecy, then for every allowable L-set of messages M' and for every L-set of source states S' there exists an encoding rule e such that $e(S') = M'$.

It is also straightforward to show:

Lemma 4.2 If an SC(k,v,b) provides U(L)-secrecy, then
$b \geq |A_L|$,
where A_L is the set of allowable L-subsets of M.

Using these Lemmas we can now establish the following theorem. Note the bound in this theorem is a special of theorem 5.3 in [DeSo1] for systems providing S(L)-secrecy.

Theorem 4.3 If an SC(k,v,b) provides U(L)-secrecy, then
$b \geq (v/k).\binom{k}{L}$,

Moreover, if $b = (v/k).\binom{k}{L}$, then:

(i) For any pair of encoding rules e_1, e_2 either
$e_1(S) = e_2(S)$
or $e_1(S)$ and $e_2(S)$ are disjoint.

(ii) If e_1 and e_2 are encoding rules satisfying
$e_1(S) = e_2(S)$
then
$p_E(e_1) = p_E(e_2) = p_M(M^*)$
for every M^* in A_L which is also a subset of $e_1(S)$.

We consider examples of schemes possessing U(L)-secrecy in section 5 below. Note that, because S(L)-secrecy implies U(L)-secrecy, the results of Theorem 4.3 also apply to S(L)-secure systems.

If we now consider O(L)-secrecy, then we get a similar set of results as follows:

Lemma 4.4 If an SC(k,v,b) provides O(L)-secrecy then for every allowable L-tuple of distinct messages $\underline{m}$ and for every L-tuple of distinct source states $\underline{s}$ there exists an encoding rule e such that
$e(\underline{s}) = \underline{m}$.

It is also straightforward to show:

Lemma 4.5 If an SC(k,v,b) provides O(L)-secrecy, then
$b \geq |O_L|$,
where O_L is the set of allowable L-tuples of distinct elements of M.

Using these Lemmas we can now establish the following result. Note that the bound in this theorem was previously established by Massey (equation (5), [Mass1]).

Theorem 4.6 If an SC(k,v,b) provides O(L)-secrecy, then
$b \geq v.(k-1)!/(k-L)!$.
Moreover, if $b = v.(k-1)!/(k-L)!$ then:

(i) For any pair of encoding rules e_1, e_2 , either
$e_1,(S) = e_2(S)$
or $e_1,(S)$ and e_2 (S) are disjoint.
(ii) If e_1, and e_2 are encoding rules satisfying
$e_1,(S) = e_2$ (S)
then
$p_E(e_1,) = p_E(e_2) = p_M(m)$
for every m in O_L for which all elements in m are in $e_1,(S)$.

5. EXAMPLES

We will consider some examples of L-secure systems for which the numbers of encoding rules meet the lower bounds established in section 4 above. It is of interest to construct such systems since, for any security system, it is always desirable to minimise the number of encoding rules and hence the key size. We shall divide our examples into two categories; namely those satisfying the bounds of Theorems 4.3 and 4.6 respectively.

We consider (t,w) homogeneous or transitive set of permutations, Latin Square, Perpandicular Array (using results in [Mull1]), Orthogonal Arrays of Type II ([Rao1]), to characterize and to construct schemes achieving the bounds.

REFERENCES

[Bric1] E.F. Brickell, "A few results in message authentication", *Congressus Numerantium* 43 (1984) 141-154.

[DeSo1] M. De Soete, "Some constructions for authentication-secrecy codes", paper given at *Eurocrypt 88*.

[DeSo2] M. De Soete, "Bounds and constructions for authentication-secrecy codes", paper given at *Crypto 88*.

[Gilb1] E.N. Gilbert, F.J. MacWilliams and N.J.A. Sloane, "Codes which detect deception", *Bell System Technical Journal* 53 (1974) 405-424.

[Mass1] J.L. Massey, "Cryptography - a selective survey", in: *Digital Communications, editors: C. Biglieri and C. Prati*, Elsevier (North-Holland), 1986, pp. 3-21.

[Mull1] R.C. Mullin, P.J. Schellenberg, G.H.J. van Rees and S.A. Vanstone, "On the construction of perpendicular arrays", *Utilitas Mathematica* 18 (1980) 141-160.

[Rao1] C.R. Rao, "Combinatorial arrangements analogous to orthogonal arrays", *Sankhya Series A* 23 (1961) 283-286.

[Shan1] C.E. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal* 28 (1949) 656-715.

[Simm1] G. Simmons, "Authentication theory/coding theory", in: *Advances in Cryptology: Proceedings of Crypto 84*, Springer-Verlag (Berlin), 1985, pp. 411-431.

[Stin1] D.R. Stinson, "A construction for authentication/secrecy codes from certain combinatorial designs", in: *Advances in Cryptology: Proceedings of Crypto 87*, Springer-Verlag (Berlin), 1988, pp. 355-366.

[Stin2] D.R. Stinson, "Some constructions and bounds for authentication codes", *Journal of Cryptology* 1 (1988) 37-51.