Journal of Universal Computer Science, vol. 2, no. 5 (1996), 347-379
submitted: 13/5/96, accepted: 13/5/96, appeared: 28/5/96 © Springer Pub. Co.

TOWARDS FOUNDATIONS OF CRYPTOGRAPHY: INVESTIGATION OF PERFECT SECRECY[1]

H. Jürgensen[2] **L. Robbins**[2]

Abstract

In the spirit of Shannon's theory of secrecy systems we analyse several possible natural definitons of the notion of perfect secrecy; these definitions are based on arguments taken from probability theory, information theory, the theory of computational complexity, and the theory of program-size complexity or algorithmic information. It turns out that none of these definitions models the intuitive notion of perfect secrecy completely: Some fail because a cryptographic system with weak keys can be proven to achieve perfect secrecy in their framework; others fail, because a system which, intuitively, achieves perfect secrecy cannot be proven to do so in their framework.

To present this analysis we develop a general formal framework in which to express and measure secrecy aspects of information transmission systems.

Our analysis leads to a clarification of the intuition which any definition of the notion of perfect secrecy should capture and the conjecture, that such a definition may be impossible, that is, that only secrecy by degrees can be defined rigorously.

This analysis also leads to a clarification of what the cryptographic literature refers to as the one-time pad. On the basis of the arguments used for its strength in the literature, one has to distinguish between two quite different systems: the first kind uses randomly chosen strings of some given length; the second kind uses random strings, that is, patternless strings of some given length. The former achieves perfect secrecy in the sense of Shannon, but permits weak keys – like the all-zero key; the latter, while intuitively stronger, does not achieve perfect secrecy in any of the proposed senses.

Finally, the analysis exposes the need for a formal, non-operational, but mathematical definition of the notion of weak key.

Keywords: cryptography, perfect secrecy, program-size complexity, information theory, computational complexity.

[1] C. Calude (ed.). *The Finite, the Unbounded and the Infinite, Proceedings of the Summer School "Chaitin Complexity and Applications,"* Mangalia, Romania, 27 June – 6 July, 1995. The research reported in this paper was supported by the Natural Sciences and Engineering Council of Canada, Grant OGP0000243.

[2] Department of Computer Science, The University of Western Ontario, London, Ontario, Canada, N6A 5B7. Electronic mail: helmut@uwo.ca, lynda@csd.uwo.ca.

1. Introduction

Security systems for information processing are used to protect information against unauthorized access – passive access like mere reading of the information, or active access like modification of the information. Protocols and cryptographic systems are among the main components of such security systems. Protocols define how system components are to be used; cryptographic systems achieve information hiding. In this paper, we analyse the limitations, in principle, of cryptographic systems. We do not address other aspects of security systems except to explain how certain issues in cryptography can be adequately treated as protocol issues.

The first general formal analysis of cryptographic systems was developed by Shannon [38]. Shannon's model is based on probability theoretic and information theoretic considerations. Some modifications of that model were proposed in [23] and [28]. The present paper is intended to be a continuation of this very basic work towards a rigorous mathematical foundation of cryptography.

In the following discussion we assume the well-known model of information transmission consisting of a source S sending information to a recipient R via a channel C as illustrated in Fig. 1.1. Before actual transmission, the information is encoded using an encoder γ and, before reception, it is decoded using a decoder δ. During transmission, the encoded information may undergo changes due to faults in the channel or environmental conditions; such faults are modelled by a source N of noise. Moreover, the information may be overheard or even altered during transmission by a hostile participant, the adversary A. In this model, S and R may, but need not be distinct physical entities, and C may represent any kind of physical channel. We consider only discrete channels which operate in discrete time steps and which use discrete signals.

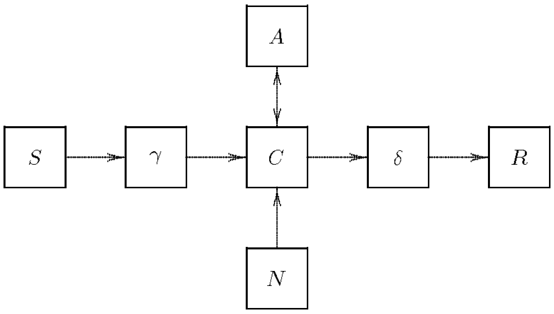

Fig. 1.1. The information processing and transmission model.

The purposes of the encoding γ and the decoding δ include the following:

- translation between the alphabets used by S, C, and R;
- reduction of the effect of noise on C;
- adaptation of the information rates at which S, C, and R operate;
- information compression;
- information security.

In this paper, we consider only the aspect of information security – specifically, that of secrecy.[3] For the other points mentioned we refer to [26] where the basic requirements of γ and δ are discussed and where further references can be found.

Intuitively, a system should be deemed to achieve *perfect secrecy* if it is *impossible* for the adversary to gain unauthorized access to the information being transmitted. This is the motivation for Shannon's definition of perfect secrecy [38]: A system achieves perfect secrecy if the a posteriori message probabilities are the same as the a priori message probabilities, that is, if by receiving the encoded message, the *cryptogram,* the adversary learns nothing about the message. We re-examine this definition and some of its variants found in the cryptographic literature keeping its intended meaning in mind.

It seems natural to require that any definition $\mathbb{S}$ of *perfect secrecy* should have to satisfy the following two conditions:

(1) No system with any cryptographic weaknesses should be said to achieve *perfect* secrecy according to $\mathbb{S}$.

(2) If a system is cryptographically unbreakable then it should be said to achieve *perfect* secrecy according to $\mathbb{S}$.

Moreover, an assertion of perfect secrecy should be *proven* according to the definition $\mathbb{S}$.

In this paper, we argue that Shannon's probability-based definition of perfect secrecy does not meet these conditions: It seems not to capture the cryptographic idea of perfect secrecy exactly, because it does not satisfy the first of the two conditions. We show that also other obvious candidates for such a definition, based on information theoretic arguments or on notions from computational or program-size complexity theory, miss some part of these requirements. We also show, in particular, that one type of argument often employed in textbooks on cryptology to prove that the so-called one-time pad achieves perfect secrecy is mathematically incorrect.

Depending on the context, the one-time pad is sometimes described as a randomly chosen string of key symbols or as a random string of key symbols. This distinction seems to be irrelevant, but is, in fact, crucial – as we point out in this paper. In the former case, the key string is chosen at random from the set of all strings of a given length; then the proof of perfect secrecy is obtained as a simple consequence of Shannon's definition as shown in Section 4 below; this case, however, includes situations which are, intuitively, not secure at all; in particular, this case does not exclude the usage of so-called weak keys. In the latter case, the key string satisfies certain randomness properties – like containing no patterns; then the proof of perfect secrecy or unbreakability is commonly based on the intuitive argument that a random string, applied as a key to a message, which is a non-random string, will result in a random string as the cryptogram; thus the adversary would have no clue regarding the message when a cryptogram is received; this argument is mathematically incorrect.[4]

[3] Other aspects of security include robustness against forging, modifying, substituting or withholding messages.

[4] See, for example, [37], p. 14, [2], pp. 243–246. Also [1], pp. 110–111 seems to

To avoid misunderstandings: we do *not* at all claim that the one-time pad or Vernam cipher is weak; it isn't. We show here that there is, so far, no acceptable general mathematical framework in which

- this cryptographic system can be proven to achieve perfect secrecy and
- all systems with weaknesses can be proven not to achieve perfect secrecy.

The problem is with the *definition* of *perfect secrecy,* not with the one-time pad.

As mentioned, the problem with Shannon's definition of perfect secrecy is that cryptographic systems with weaknesses can be proven to achieve perfect secrecy in that sense. These theoretical weaknesses result from the presence of *weak keys*.

Intuitively, a key is weak, if cryptograms obtained with it can be read by the adversary comparatively easily. For example, a key that happens to leave messages largely unchanged should be considered weak. Most cryptographic systems have weak keys and, if they are known, one avoids using them.[5]

Therefore, one could argue that the problem can be easily avoided by not using the weak keys, that is, in essence by excluding these keys from the key space defining the cryptographic system. This would be a mathematically acceptable solution if there were a rigorous definition of the notion of *weak key.* Such a definition does not exist. In fact, the definitions of these two notions, *weak key* and *perfect secrecy,* seem to hinge on each other in a vicious circle. Mathematically, it seems impossible to define one without the other. Hence, *for a mathematical model of secrecy systems,* we cannot simply ignore the existence of weak keys as a matter of how the system is used, but have to cope with them within our definitional framework. In fact, we believe that our work may ultimately lead to a proper definition of weakness in keys.

Moreover, it turns out that, with the weak keys excluded, the one-time pad can no longer be proven to achieve perfect secrecy; this is a rather counter-intuitive consequence of Shannon's definition.

As a consequence of these considerations, we examine whether it is possible at all to arrive at a cryptographically acceptable rigorous definition of perfect secrecy. We show evidence that allows us to argue that such a definition may not be possible and that secrecy, in a rigorous mathematical sense, can only be achieved by degrees in general.

We consider four different approaches to a mathematical definition of perfect secrecy – x-perfect secrecy where x is one of the letters p, i, c, and r – based on probability theory, information theory, computational complexity theory, and program-size complexity theory, respectively. In each case we expose the limitations of that notion in comparison to the two general conditions any definition of perfect secrecy ought to satisfy. To emphasize the similarity of the approaches and to clarify their differences we develop a general mathematical framework in

---

have this argument in mind. Sometimes, the argument seems to be mixed as in [37], pp. 14–15, or [34], p. 342.

[5] See, for example, [6] for the RSA system; [17], p. 372, [30], [24], p. 220, [4] for the U.S. American *data encryption standard,* the DES.

which the strengths of cryptographic systems can be expressed and evaluated from these four points of view and many others in a uniform manner.

Our paper is structured as follows. In Section 2 we review some basic notions and notation. In Section 3 we develop a general framework in which to express various aspects of cryptographic systems in a uniform fashion; the key notions introduced there are those of passive and active access potential, adversary, and cryptanalyst. Within this framework, we express Shannon's probability-theory based approach to secrecy systems [38] in Section 4; we then show that, among the cryptographic systems which can be *proven* to achieve perfect secrecy, there are some which permit the usage of cryptographically very weak keys. In Section 5, we examine Shannon's information theoretic approach to secrecy and point out some of its limitations. This is followed by a very brief discussion of secrecy from the point of view of computational complexity in Section 6. In Section 7, we examine the second notion of one-time pad, mentioned above, from the point of view of program-size complexity. We exhibit an error in the usual argument employed to prove that it is unbreakable. Summarizing, in Section 8, we argue the impossibility of a satisfactory definition of perfect secrecy; moreover, we show that even a natural definition of degree of secrecy may be very difficult to obtain.

All this does not mean that the one-time pad is not secure to use. It just means that there is no proof of its strength because there is no convincing definition of perfect secrecy.

In this paper we only consider private-key cryptographic systems. In Section 3 we briefly indicate how public-key systems fit into the same framework. In the context of this paper and at this level of generality, the distinction between public and private key, albeit very important in practice, is of no consequence.

Some thoughts expressed in this paper may be highly controversial because they challenge long-standing beliefs in cryptology. They grew out of an attempt to put the often cryptic explanations of perfect secrecy in textbooks on cryptology onto a firm mathematical basis. We found – to our surprise – that such a firm basis may not be achievable.

2. Notation and Basic Notions

In this section we introduce the notation to be used and we review some basic notions.

The symbol $\mathbb{N}$ denotes the set of positive integers, and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. $\mathbb{Z}$ and $\mathbb{R}$ denote the sets of integers and reals, respectively. Let $\mathbb{B}$ denote the set $\{0, 1\}$ of Boolean values. Occasionally, we identify $\mathbb{B}$ with the field GF(2) with two elements; the operation $\oplus$ of *exclusive or* in $\mathbb{B}$ corresponds to addition in GF(2).

An *alphabet* is a non-empty, finite set. In the sequel, we assume without special mention that all alphabets used in this paper contain at least the two distinct elements 0 and 1. Let X be an alphabet. Then X^* denotes the set of all *strings* (or *words*) over X, including the empty string ε. Let $X^+ = X^* \setminus \{\varepsilon\}$. By X^ω we denote the set of *infinite strings* (or ω*-words*) over X. Let $X^\infty = X^* \cup X^\omega$. For $w \in X^\infty$, let $|w| \in \mathbb{N}_0 \cup \{\infty\}$ be the *length* of w. For $n \in \mathbb{N}_0$, let X^n be the set of all strings of length n over X. For a string $u \in X^\infty$ and $n \leq |w|$, let $\mathrm{pref}_n(u)$ be the prefix of length n of u, that is, $|\mathrm{pref}_n(u)| = n$ and $u \in \mathrm{pref}_n(u)X^\infty$.

Let $<$ be an arbitrary, but fixed total order on X. Let $u = u_1u_2\cdots u_n$ and $v = v_1v_2\cdots v_m$ with $u_i, v_j \in X$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$. Assume that $u \neq v$. We extend $<$ to X^* as follows:

(1) If $n < m$ then $u < v$; if $m < n$ then $v < u$.

(2) If $n = m$, let k be maximal such that $u_1u_2\cdots u_k = v_1v_2\cdots v_k$. Then $0 \leq k < n$ and $u_{k+1} \neq v_{k+1}$. If $u_{k+1} < v_{k+1}$ then $u < v$. Otherwise, $v < u$.

This order on X^* is called the *quasi-lexicographic* order on X^*. For $n \in \mathbb{N}$, let $\mathrm{str}(n)$ be the nth string with respect to the quasi-lexicographic order. In particular, $\mathrm{str}(1) = \varepsilon$.

If S is a set then $|S|$ is its cardinality, 2^S is the set of all subsets of S, and id_S is the identity mapping of S. For sets S and T, S^T denotes the set of all mappings of T into S.

For sets S, T, and R and a partial mapping φ of $S \times T$ into R, $\lambda s.[\varphi(s,t)]$ denotes the partial mapping of S into R when $t \in T$ is fixed. This λ-notation is adapted to the situation as required. To indicate that φ is a partial mapping, we write $\varphi : S \times T \xrightarrow{\circ} R$. The notation $\varphi : S \times T \to R$ implies that φ is a total mapping.

If α is a relation, $\alpha \subseteq S \times T$, then, for $s \in S$,

$$\alpha(s) = \{t \mid t \in T, (s,t) \in \alpha\}$$

and, for $t \in T$,

$$\alpha^{-1}(t) = \{s \mid s \in S, (s,t) \in \alpha\};$$

moreover,

$$\mathrm{dom}\alpha = \{s \mid s \in S, \exists t \in T\ (s,t) \in \alpha\}$$

and

$$\mathrm{im}\alpha = \{t \mid t \in T, \exists s \in S\ (s,t) \in \alpha\}.$$

The sets $\mathrm{dom}\alpha$ and $\mathrm{im}\alpha$ are the *domain* and the *image* of α, respectively.

Let S be a set. Then $\mathrm{Seq}S$ denotes the set of finite *sequences* (tuples) of elements in S, including the *empty sequence* $(\,)$. For $s \in \mathrm{Seq}S$, let $\mathrm{last}(s)$ be the last element of s, when $s \neq (\,)$, and the empty sequence $(\,)$, when $s = (\,)$. For $s \in \mathrm{Seq}S$ and $e \in S$, let $\mathrm{app}(s,e)$ be the sequence obtained from s by appending e to s as the last element. Thus $\mathrm{last}(\mathrm{app}(s,e)) = e$.

Let S be a set. An *outer measure* [22] on S is a mapping $\sigma : 2^S \to \mathbb{R} \cup \{\infty\}$ satisfying the following conditions:

(a) $\sigma(\emptyset) = 0$.

(b) If $S' \subseteq S'' \subseteq S$ then $\sigma(S') \leq \sigma(S'')$.

(c) If $(S_i)_{i\in I}$ is a family of subsets of S with $I \subseteq \mathbb{N}$, then

$$\sigma(\bigcup\nolimits_{i\in I} S_i) \leq \sum\nolimits_{i\in I} \sigma(S_i).$$

Note that (c) implies that $\sigma(S') \geq 0$ for all $S' \subseteq S$. Examples of outer measures include cardinality and probability. As usual, we assume that $\infty + x = x + \infty = \infty$ for all $x \in \mathbb{R}$.

Let S be a finite, non-empty set and let p be a probability on S. The *entropy* of the probability space $\mathcal{S} = (S, p)$ is given by $H(S) = \sum_{s \in S} -p(s) \log p(s)$. One sets $0 \log 0 = 0$ using the fact that $\lim_{x \to +0} x \log x = 0$. All logarithms are taken at base 2 in this paper. The entropy can be interpreted as the average amount of uncertainty about the outcome of an experiment in $\mathcal{S}$ or as the average information contained in an event in $\mathcal{S}$. If $\mathcal{S}$ is a product space, $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2$ with $\mathcal{S}_1 = (S_1, p_1)$ and $\mathcal{S}_2 = (S_2, p_2)$ then one defines the conditional entropy of $\mathcal{S}_1$ given $s_2 \in S_2$ as $H(S_1 \mid s_2) = \sum_{s_1 \in S_1} -p(s_1 \mid s_2) \log p(s_1 \mid s_2)$. Thus $H(S_1 \mid s_2)$ is the average uncertainty about the outcome of an experiment in $\mathcal{S}_1$ when the outcome in $\mathcal{S}_2$ is known to be s_2. Finally, $H(S_1 \mid S_2) = \sum_{s_2 \in S_2} p(s_2) H(S_1 \mid s_2)$ is the conditional entropy of S_1 given S_2.

Depending on the context, we consider sets as abstract entities or as *represented sets.* A represented set is a subset of X^∞ for a suitable alphabet X. When notions like *computability* or *recursivity* are involved, we assume that all sets in question are represented. When using partial recursive functions, in this paper, we only consider such partial recursive functions that map finite strings onto finite strings. An extension of the results of this paper to infinite strings[6] is possible and requires some careful topological and measure theoretic considerations (see [41] and [13]).

3. Cryptographic Systems

In this section we introduce the notion of a cryptographic system. The formalism is influenced by the work in [28] and [27]. Our definitions are much more general than required for any implementation of a cryptographic system. They are meant to provide the general uniform conceptual framework for the restricted and more realistic definitions in subsequent sections, according to the respective focus of the analysis.

Definition 3.1 An *information transmission system* is a quintuple

$$(M, K, E, \gamma, \delta)$$

such that M, K, and E are sets, γ is a partial mapping of $M \times K$ into E, δ is a partial mapping of $E \times K$ into M with the following properties:

(1) For every $m \in M$ there is $k \in K$ such that $(m, k) \in \mathrm{dom}\gamma$.

(2) For every $m \in M$ and every $k \in K$, if $(m, k) \in \mathrm{dom}\gamma$, then $(\gamma(m, k), k) \in \mathrm{dom}\delta$ and $\delta(\gamma(m, k), k) = m$.

(3) For every $e \in E$ there exist $m \in M$ and $k \in K$ such that $(m, k) \in \mathrm{dom}\gamma$ and $\gamma(m, k) = e$.

The set M is said to be the set of *messages,* K is the set of *keys,* and E is the set of *encoded messages.* The mapping γ is the *encoding* and the mapping δ is the *decoding.*

An information system $(M, K, E, \gamma, \delta)$ is said to be *finite* when M and K are finite.

[6] This generalization is of extreme interest as it models the situation when the beginning or the end of a message are unknown.

In Definition 3.1, we do not specify how M, K, and E are represented, nor do we make any assumptions about computational or secrecy properties of γ and δ. Condition (1) guarantees that every message can be encoded. Condition (2) ensures that a message encoded using a key k can be recovered from the encoding using that key again. By condition (3), E is precisely the set of encoded messages.

The term *key* seems to suggest cryptography; in our general framework, however, a key is just a parameter determining which encoding and decoding to select. For example, in electronic file transmission, the key may just indicate whether a conversion of binary to ASCII is to be applied prior to transmission; of course the recipient then has to know whether to apply the inverse conversion or not. Thus, *per se* the term *key* has no implications for secrecy.

We use the terms *encoding* and *decoding* in their general meanings of mapping; in cryptography, these mappings are usually called *encryption* and *decryption,* respectively, and the term *code* is reserved for a very special cryptographic technique (see [29], for example). On the other hand, in coding theory, these terms usually imply certain special algebraic properties (see [26], for example).

In Definition 3.1, the encoding γ and the decoding δ use the same keys. To decode a $\gamma(m, k)$, δ uses[7] the key k. This is not really a restriction. Suppose there is a set K_γ of keys for the encoding γ and set K_δ for the decoding δ; then, to achieve the goal of information transmission, there must be a mapping κ of K_γ into K_δ such that $\delta(\gamma(m, k), \kappa(k)) = m$ for all $m \in M$ and $k \in K$ such that $(m, k) \in \mathrm{dom}\gamma$. Now let $K = \{(k_\gamma, \kappa(k_\gamma)) \mid k_\gamma \in K_\gamma\}$ and consider $k = (k_\gamma, \kappa(k_\gamma)) \in K$. Define $\gamma' : M \times K \to E$ and $\delta' : E \times K \to M$ by $\gamma'(m, k) = \gamma(m, k_\gamma)$ and $\delta'(e, k) = \delta(e, \kappa(k_\gamma))$, respectively. Then $(M, K, E, \gamma', \delta')$ is an information transmission system in the sense of Definition 3.1.

Thus, whether the encoding and decoding use the same or different keys is not a matter of the system itself, but of how it is used, that is, it is a protocol matter. In particular, this shows that *public-key cryptographic systems* fall into the realm of Definition 3.1. This means that, at the level of generality assumed in this paper, we do not need to distinguish between public-key and private-key cryptographic systems.

Example 3.1 Let $X = \{0, 1\}$, $M \subseteq X^\infty$, $K \subseteq X^\infty$, and for $m \in M$ and $k \in K$ let $(m, k) \in \mathrm{dom}\gamma$ if and only if $|m| = |k|$. Let $\oplus$ denote the binary operation on X given by

$$a \oplus b = \begin{cases} 0, & \text{if } a = b, \\ 1, & \text{if } a \neq b. \end{cases}$$

Clearly, when X is identified with $\mathbb{B}$ then $\oplus$ is the exclusive-or operation; when X is identified with GF(2) then $\oplus$ is the addition in this field. We extend $\oplus$ to $\bigcup_{i \in \mathbb{N}_0 \cup \{\omega\}} X^i \times X^i$ componentwise. For $(m, k) \in \mathrm{dom}\gamma$, let

$$\gamma(m, k) = m \oplus k$$

---

[7] Of course, there may be a key k' which is equivalent to k, that is $\lambda m.[\gamma(m, k)] = \lambda m.[\gamma(m, k')]$ and $\lambda e.[\delta(e, k)] = \lambda e.[\delta(e, k')]$. But this is not essential for the analysis in this paper.

and

$$E = \gamma(M, K) = \{e \mid \exists m \in M \exists k \in K\, (|m| = |k| \wedge e = m \oplus k)\}.$$

Then $|\gamma(m,k)| = |m| = |k|$. Thus, we need $(e,k) \in \mathrm{dom}\delta$ if and only if $|e| = |k|$. In this case, let

$$\delta(e,k) = e \oplus k.$$

Then, for $(m,k) \in \mathrm{dom}\gamma$, one has

$$\delta(\gamma(m,k),k) = m$$

as required. With appropriate choices of M and K, this system (M,K,E,γ,δ) is the *one-time pad.*

An *adversary* to an information transmission system has the potential of *unauthorized information access,* which would affect encoded messages. We distinguish between *passive access,* the decoding of encoded messages, and *active access,* the withholding, modification, or substitution of encoded messages. For the purposes of this paper, an adversary is characterized by the potential for these types of access. We describe both, active and passive access potentials, by relations.

Definition 3.2 Let $\mathfrak{I} = (M,K,E,\gamma,\delta)$ be an information transmission system. A *passive access potential* of $\mathfrak{I}$ is a relation $\alpha_{\mathrm{p}} \subseteq E \times M$ such that $(e,m) \in \alpha_{\mathrm{p}}$ implies that there is a key $k \in K$ with $(m,k) \in \mathrm{dom}\gamma$ and $\gamma(m,k) = e$. Let $A_{\mathrm{p}}(\mathfrak{I})$ be the set of passive access potentials of $\mathfrak{I}$.

In the sequel, we write $(m \mid e)$ instead of (e,m) for $(e,m) \in \alpha_{\mathrm{p}}$; this is to be read as *m given e.*

Lemma 3.1 *The set $A_{\mathrm{p}}(\mathfrak{I})$ of passive access potentials of an information transmission system $\mathfrak{I}$ is a complete lattice with respect to union and intersection; moreover, it is closed under taking subsets.*

Let $\mathfrak{I} = (M,K,E,\gamma,\delta)$ be an information transmission system. Because of Lemma 3.1, the relation

$$\alpha_{\mathrm{p}}^{\mathrm{full}} = \bigcup_{\alpha_{\mathrm{p}} \in A_{\mathrm{p}}(\mathfrak{I})} \alpha_{\mathrm{p}}$$

is a passive access potential. It is the maximal element of $A_{\mathrm{p}}(\mathfrak{I})$. We call it the *full passive access potential* of $\mathfrak{I}$.

Suppose $\alpha_{\mathrm{p}} \in A_{\mathrm{p}}(\mathfrak{I})$. Then $(m \mid e) \in \alpha_{\mathrm{p}}$ is intended to express the fact that an adversary, upon seeing e transmitted, could determine m as the message having been sent. In particular, the relation $\alpha_{\mathrm{p}}^{\mathrm{full}}$ describes the *a priori* knowledge available about messages and corresponding encoded messages from the very definition of the information transmission system under considertion, because

$$\alpha_{\mathrm{p}}^{\mathrm{full}} = \{(m \mid e) \mid \exists k \in K\ \gamma(m,k) = e\}.$$

If no other information is available then, intuitively, the size of the sets $\alpha_{\mathrm{p}}^{\mathrm{full}}(e)$ with $e \in E$ could be a criterion for *passive access security.* When $\alpha_{\mathrm{p}}^{\mathrm{full}}(e)$ is large for every $e \in E$, then an adversary has too much choice among the many messages m with $(m \mid e) \in \alpha_{\mathrm{p}}^{\mathrm{full}}$.

Additional considerations may lead one to consider a proper subset α_{p} of $\alpha_{\mathrm{p}}^{\mathrm{full}}$ as the passive access potential of a typical adversary. This might reflect limitations of the cryptanalytic resources available to the adversary; it could also reflect a special interest or expectation of the adversary – expecting messages about financial transactions and ignoring everything else, for example. Again intuitively, passive access security decreases when sets $\alpha_{\mathrm{p}}(e)$ are small, but non-empty for many $e \in E$; on the other hand, it increases if $\alpha_{\mathrm{p}}(e) = \emptyset$ for many $e \in E$. The former says that the message corresponding to a given encoded message is nearly unique and, therefore, the adversary can assume that it is the true message with some confidence; the latter says, that the adversary does not know any message at all to associate with an encoded message e.

Definition 3.3 Let $\mathfrak{I} = (M, K, E, \gamma, \delta)$ be an information transmission system. A *passive access measure* is an outer measure μ on E. A *unicity measure* is a mapping υ of E into the set of outer measures on M.

We use a passive access measure μ and a unicity measure υ as follows to measure the security of an information transmission system $\mathfrak{I} = (M, K, E, \gamma, \delta)$ with respect to unauthorized passive information access. Let $\alpha_{\mathrm{p}} \in A_{\mathrm{p}}(\mathfrak{I})$ be a passive access potential; it describes the information a given adversary could access in principle on the basis of intercepting encoded messages.

By μ we measure the size of the set $\mathrm{dom}\alpha_{\mathrm{p}}$ of all encoded meassages e for which $\alpha_{\mathrm{p}}(e)$ is non-empty. If $\mu\,(\mathrm{dom}\alpha_{\mathrm{p}})$ is 0 then the adversary described by α_{p} cannot obtain any original messages from encoded messages – in the sense of μ. On the other hand, if $\mu\,(\mathrm{dom}\alpha_{\mathrm{p}})$ is large, then, in the sense of μ, then there are many encoded messages for which the adversary can obtain some originals. The former case means security; the latter case indicates potential insecurity.

By υ we measure the size of the sets $\alpha_{\mathrm{p}}(e)$ for $e \in E$, that is $\upsilon(e)(\alpha_{\mathrm{p}}(e))$. We distinguish three cases. If $\upsilon(e)(\alpha_{\mathrm{p}}(e)) = 0$ then – in the sense of $\upsilon(e)$ – the adversary cannot recover any original message from the encoded message e. If $\upsilon(e)(\alpha_{\mathrm{p}}(e))$ is very large then the adversary, given e, will not be able to determine which among the many messages in $\alpha_{\mathrm{p}}(e)$ is the true original one. Finally, if $\upsilon(e)(\alpha_{\mathrm{p}}(e))$ is non-zero, but small – for example, smaller than some pre-determined threshold –, then the adversary may be able to determine the original message from e with some confidence. The first case indicates absolute secrecy of e; the second case indicates a certain level of secrecy for e; the last case indicates the potential for lack of secrecy.

From the point of view of the system users, $\mu\,(\mathrm{dom}\alpha_{\mathrm{p}})$ should be 0 or at least very small; this would imply that $\alpha_{\mathrm{p}}(e) = \emptyset$ for all or nearly all $e \in E$ – as measured by μ. For those $e \in E$ with $\alpha_{\mathrm{p}}(e) \neq \emptyset$, the value of $\upsilon(e)(\alpha_{\mathrm{p}}(e))$ should be 0 or very large. The adversary would wish to face the opposite situation: $\mu\,(\mathrm{dom}\alpha_{\mathrm{p}})$ as large as possible and $\upsilon(e)(\alpha_{\mathrm{p}}(e))$ non-zero, but small, for as many $e \in E$ as possible.

In particular, we can use the cardinality as outer measure. Other outer measures are considered in Sections 4 and 5 below. Let $\mu_{|\,.\,|} = \lambda x.[\,|x|\,]$ be this passive access measure. Moreover, let $\upsilon_{|\,.\,|} = \lambda e.[\lambda x.[\,|x|\,]]$; thus υ assigns, to every $e \in E$, cardinality as the outer measure on M. Then $\mu_{|\,.\,|}(\mathrm{dom}\alpha_{\mathrm{p}})$ is the number of encoded messages $e \in E$ such that $(m \mid e) \in \alpha_{\rm p}$ for some $m \in M$, that is, the number of encoded messages which the adversary is able to read in principle. Moreover, for $e \in E$, $\upsilon_{|\,.\,|}(e)(\alpha_{\rm p}(e))$ is the number of possible messages $m \in M$ that the adversary could determine from e. From the point of view of security, the best situation is when $\mu_{|\,.\,|}(\mathrm{dom}\alpha_{\rm p})$ is as small as possible; then the adversary can read only very few encoded messages. Moreover, whenever $\alpha_{\rm p}(e) \neq \emptyset$ then there should be a very large number of messages such that $m \in \alpha_{\rm p}(e)$, that is, $\upsilon_{|\,.\,|}(e)$ should be very large.

An extreme case occurs when $\alpha_{\rm p}(e) = M$ for all $e \in E$. This happens, for instance, with the system of Example 3.1 using $M = K = E = X^n$ for some $n \in \mathbb{N}$. Then, for every $e \in E$ and every $m \in M$ there is a (unique) $k \in K$ such that $m \oplus k = e$, hence $\alpha_{\rm p}^{\rm full}(e) = M$. Without any other information than e, the cryptanalyst has no clue as to which m to choose. This is one of the reasons for the strength of a cryptographic system like this one, the one-time pad.

Unauthorized active information access occurs when an adversary sends an encoded message to the recipient which differs from the original; in fact, a message may even be sent when no original exists. We model active access also by a relation.

Let $\mathfrak{I} = (M, K, E, \gamma, \delta)$ be an information transmission system. Let $\diamond$ be a symbol (element) not contained in E, and let $E_\diamond = E \cup \{\diamond\}$. We use $\diamond$ to represent the absence of an (encoded) message. For simplicity, we now also refer to the elements of $E_\diamond$ as encoded messages. At time $t \in \mathbb{N}_0$ a sequence $s_t \in \mathrm{Seq}E_\diamond$ will represent the information traffic seen by the adversary up to and including time t. Initially, the adversary has not seen anything; we represent this by $s_0 = (\,)$. If the adversary has seen s_t and, at time $t+1$, the encoded message $e_{t+1} \in E_\diamond$ is observed, then $s_{t+1} = \mathrm{app}(s_t, e_{t+1})$. Based on what the adversary has seen at any given time, he or she may taken certain actions. This motivates the following definition of active information access potential.

Definition 3.4 Let $\mathfrak{I} = (M, K, E, \gamma, \delta)$ be an information transmission system. An *active access potential* of $\mathfrak{I}$ is a relation $\alpha_{\rm a} \subseteq \mathrm{Seq}E_\diamond \times E_\diamond$ such that, for all $e \in E_\diamond$ and for all $s \in \mathrm{Seq}E_\diamond$, if $\mathrm{last}(s) = e$ then $(s, e) \in \alpha_{\rm a}$. Let $A_{\rm a}(\mathfrak{I})$ be the set of active access potentials of $\mathfrak{I}$.

Again, for $(s, e) \in \alpha_{\rm a}$, we write $(e \mid s)$ instead of (s, e); this is to be read as *e given s.*

If $\alpha_{\rm a}$ is the active access potential of an adversary, then $(e \mid s) \in \alpha_{\rm a}$ is intended to mean that the adversary, having seen the sequence s of encoded messages, could send the encoded message e to the recipient. The requirement that $(e \mid s) \in \alpha_{\rm a}$ whenever $\mathrm{last}(s) = e$ means that the adversary can always let the encoded message pass unchanged.

In particular, Definition 3.4 includes the case of $(e \mid s) \in \alpha_{\rm a}$ with $\mathrm{last}(s) = \diamond$ as a possibility. In such a case, the adversary could send e to the recipient, pretending this originates with the sender, without there having been a message from the sender. Definition 3.4 also includes the case of $(\diamond \mid s)$ with $\mathrm{last}(s) \neq \diamond$. This means that the adversary could simply withhold the encoded message $\mathrm{last}(s)$.

In principle, unauthorized active information access does not imply that the adversary knows the original messages. It may be sufficient for the adversary just to observe the message traffic – or its absence – to decide what to send to the recipient.

Unauthorized active information access could be considered as *noise* on the transmission channel. Instead of the correct $\gamma(m,k)$ or $\diamond$, the recipient gets some $e \in E_\diamond$ such that $(e \mid s) \in \alpha_{\mathrm{a}}$ and $\mathrm{last}(s) = \gamma(m,k)$ or $\mathrm{last}(s) = \diamond$.

Lemma 3.2 *The set $A_{\mathrm{a}}(\mathfrak{I})$ of active access potentials of an information transmission system is a complete lattice with respect to union and intersection. Its minimal element is the relation*

$$\alpha_{\mathrm{a}}^{\min} = \left\{(e \mid s) \mid e \in E_\diamond, s \in \mathrm{Seq}E_\diamond, \mathrm{last}(s) = e\right\}.$$

The active access potential $\alpha_{\mathrm{a}}^{\min}$ indicates that the adversary cannot remove, change, or insert encoded messages, that is, the encoded messages are simply passed on to the recipient. The other extreme is

$$\alpha_{\mathrm{a}}^{\max} = \bigcup_{\alpha_{\mathrm{a}} \in A_{\mathrm{a}}(\mathfrak{I})} \alpha_{\mathrm{a}} = \{(e \mid s) \mid s \in \mathrm{Seq}E_\diamond, e \in E_\diamond\}.$$

An adversary with $\alpha_{\mathrm{a}}^{\max}$ could send any encoded message at any time without considering the observed traffic.

Definition 3.5 Let $\mathfrak{I} = (M, K, E, \gamma, \delta)$ be an information transmission system. An *adversary* for $\mathfrak{I}$ is a pair $(\alpha_{\mathrm{p}}, \alpha_{\mathrm{a}}) \in A_{\mathrm{p}}(\mathfrak{I}) \times A_{\mathrm{a}}(\mathfrak{I})$. An adversary is said to be *passive* if $\alpha_{\mathrm{a}} = \alpha_{\mathrm{a}}^{\min}$. Otherwise, the adversary is said to be *active.*

We have, so far, avoided to introduce or use terms like *cryptogram, cryptanalyst,* or *cryptanalysis* as these terms tend to imply specific implementations of information transmission systems in which the adversary's access potentials are limited by specific cryptographic techniques and in which the adversary realizes the access potentials by cryptanalytic techniques. Cryptographic techniques are used primarily to reduce the passive access potential of an adversary in terms of the chosen passive access measure μ and the chosen unicity measure υ.

In contrast to passive access, in the context of cryptographic techniques, active access is mainly controlled through protocols, that is, which messages to send in which order and how to apply the cryptographic techniques. In this paper, we focus exclusively on passive access.[8] Therefore, in the rest of this paper, an *adversary* is a *passive adversary,* and we write α_{p} instead of $(\alpha_{\mathrm{p}}, \alpha_{\mathrm{a}}^{\min})$.

Definition 3.6 Let $\mathfrak{I}$ be an information transmission system. A *cryptanalyst* for $\mathfrak{I}$ is a triple $(\alpha_{\mathrm{p}}, \mu, \upsilon)$ where $\alpha_{\mathrm{p}} \in A_{\mathrm{p}}(\mathfrak{I})$ is a passive access potential, μ is a passive access measure, and υ is a unicity measure such that $\upsilon(e)(m) > 0$ implies $(m \mid e) \in \alpha_{\mathrm{p}}$.

[8] Fundamental issues concerning protocols are analysed in [36].

With this definition of a cryptanalyst as a triple $(\alpha_{\mathrm{p}}, \mu, \upsilon)$, we capture the following intuition. In α_{p} we express, what is cryptanalysable in principle given the respective assumptions about the resources available to the adversary; μ and υ measure the secrecy achived by the system.

In the sequel, by *cryptanalyst* we usually refer to Definition 3.6, but sometimes we use the term in the more colloquial sense of a person – an adversary – attempting unauthorized reading of encoded messages; this latter process is referred to as *cryptanalysing* or *cryptanalysis.* The encoded messages are called *cryptograms.* The term *unbreakable* is used to convey the intuitive notion of cryptanalysis being impossible absolutely and without exception. Similarly, we often use the term *adversary* in its intuitive rather than its formal sense when no confusion is possible.

In cryptography, one usually makes a few basic assumptions:

- The adversary *knows* the complete information transmission system $\mathfrak{I}$. Thus, if an adversary $\alpha_{\mathrm{p}} \in A_{\mathrm{p}}(\mathfrak{I})$ knows or can obtain the key k in use, then $(m \mid e) \in \alpha_{\mathrm{p}}$ for any $m \in M$ and $e \in E$ such that $(m, k) \in \mathrm{dom}\gamma$ and $\gamma(m, k) = e$. In principle, the adversary could obtain arbitrary large subsets of $\alpha_{\mathrm{p}}^{\mathrm{full}}$.
- The adversary's resources for cryptanalysis are at least as powerful as the resources available to the sender and the recipient for information transmission.
- Unauthorized access to transmitted information may have a value which is time-dependent, that is, such access may be very valuable for the adversary and very costly for the sender or the recipient; and this value or cost may change – typically decrease – over time.
- Encoding and decoding – encryption and decryption – are computable. Cryptanalysis is also an algorithmic process. All three processes have costs: To facilitate communication, the cost of encoding and decoding should be small; to strengthen secrecy, the cost of cryptanalysis should be large. The cost analysis has to take into account the available resources.
- Some information available to the sender or the recipient has to be kept secret from the adversary. This information is part of the key.

These assumptions address two kinds of issues: First, they address how to assess the strength of a given system; for instance, the first assumption takes the very pessimistic view that the adversary can know everything in principle, this only mitigated by the fact that the resources available may be bounded. On the other hand, they also address how to use the system; for example, the last assumption points to protocol issues, that is, how to deal with keys.

In keeping with Shannon's model, we exclude protocol issues from consideration, that is, we assume that protocols are used correctly throughout.

In subsequent sections of this paper, we equip information transmission systems with additional structure which entails more structure for passive and active access potentials and for adversaries.

4. Probabilistic Aspects

Cryptanalysts are not easily discouraged by large numbers. As is well known, in a true cryptanalytic situation, the fact that $|\alpha_{\mathrm{p}}^{\mathrm{full}}(e)|$ is large for all $e \in E$ means very little. Using cardinality as the unicity measure is unrealistically optimistic.

Example 4.1 Consider the alphabet[9]

$$\begin{aligned} X = &\{A, B, \ldots, Z, a, b, \ldots, z, \sqcup\} \cup \{,\} \\ &\cup \{., !, ?, ”, “, ’, ‘, ;, :, \text{-}, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \end{aligned}$$

of symbols usually occuring in English printed text. Here $\sqcup$ denotes the space character. Thus $|X| = 74$. Let $M \subseteq X^*$ be the set of strings over X which are grammatically correct English texts. To make each $m \in M$ have a length which is divisible by 3, we add one or two characters $\sqcup$ to the end of the text. Thus $M \subseteq (X^3)^*$. Let K be the set of permutations of X^3. For $m = m_1 m_2 \cdots m_{3n} \in M$ and $k \in K$, let

$$\gamma(m, k) = k(m_1 m_2 m_3) \cdots k(m_{3n-2} m_{3n-1} m_{3n}).$$

Then $E = \gamma(M, K) \subseteq (X^3)^*$. Let

$$\delta(e, k) = k^{-1}(e_1 e_2 e_3) \cdots k^{-1}(e_{3n-2} e_{3n-1} e_{3n})$$

for $e = e_1 e_2 \cdots e_{3n} \in E$. Clearly, $\mathfrak{I} = (M, K, E, \gamma, \delta)$ is an information transmission system. For every message $m \in M$, there are $74^3!$ possible encoded messages. If $e = \gamma(m, k)$ then, without any detailed analysis, one can only state that $|\alpha_{\mathrm{p}}^{\mathrm{full}}(e)| \leq |K|$, that is, any key could have been used to get e. This is discouraging, but deceivingly so – as the history of cryptography shows (see [29]).

The cryptanalyst utilizes the fact that M consists of grammatically correct English texts. Thus, only a key k such that $\delta(e, k)$ is a correct English text could have been used. Utilizing knowledge about correct English texts, one can eplore the space of the $74^3!$ keys that could have been used much more efficiently than by just trying every key, one after the other.

While $74^3!$ is a formidable number – it is more than[10] $2^{4,000,000}$ – and trying out all keys would take for ever – at the rate of one nsec per key it would take more than 32, 000, 000 years – breaking this system is really quite easy. The cryptanalyst uses the known properties of M.

Based on centuries-old cryptographic experience and in the spirit of Example 4.1, one adds probabilistic considerations to information transmission systems.

---

[9] This is not intended to be real cryptographical example – in classical cryptography many of the symbols listed would be omitted from the start. It is meant to clarify a point.

[10] This is really a very rough estimate; but for our argument the details do not matter.

Definition 4.1 A *p-information transmission system* is a quintuple

$$(\mathcal{M}, \mathcal{K}, \mathcal{E}, \gamma, \delta)$$

such that $\mathcal{M}$, $\mathcal{K}$ and $\mathcal{E}$ are discrete probability spaces (M, p_M), (K, p_K) and (E, p_E), respectively, and $(M, K, E, \gamma, \delta)$ is an information transmission system. Moreover, for $e \in E$, one has

$$p_E(e) = \sum_{\substack{m \in M, k \in K \\ \gamma(m,k)=e}} p_{M\times K}(m, k).$$

To keep matters simple we assume, in this chapter, that M and K are countable.[11] Then also E is countable.

Moreover, it is common to assume that $\mathcal{M}$ and $\mathcal{K}$ are independent. This assumption is reasonable, as sender and recipient have to agree on a key before it is known which message will be sent. Their choice of the key may depend on the general structure of $\mathcal{M}$, but not on the choice of $m \in M$. Under this assumption, for $e \in E$, one has

$$p_E(e) = \sum_{\substack{m \in M, k \in K \\ \gamma(m,k)=e}} p_M(m)p_K(k).$$

In the sequel, we refer to this assumption as the *independence assumption.*

The following definition of p-cryptanalyst is motivated by Shannon's considerations of the probabilistic aspects of cryptographic secrecy in [38]; his information theoretic analysis is discussed in the next section.

Shannon's idea is, essentially, as follows: A cryptogram e received by the adversary, may change the adversary's assessment of message probabilities; prior to the receipt of e, the probability of a message m is $p_M(m)$ whereas, after receipt, it is $p_{M|E}(m \mid e)$, the *a posteriori* probability of m given e. Differences between these two probabilities may permit the adversary to draw conclusions about the message that has been sent. Therefore, Shannon defines that a system achieves perfect secrecy if

$$p_M(m) = p_{M|E}(m \mid e)$$

for all m and e. The idea is that receipt of the cryptogram has given the adversary no information about the message that was not available before. To embed this definition in our general framework, we modify it; however, the modifications are such that a system achieves perfect secrecy in Shannon's sense if and only if it achieves perfect secrecy in our sense. To distinguish the various possible definitions of *perfect secrecy* we prefix the word *perfect* by letters indicating the respective contexts.

[11] The generalization to uncountable M and K (with some reasonable topological structure) is not difficult, but unnecessarily complicated for the point to be made in this paper.

Definition 4.2 Let $\mathfrak{I} = (\mathcal{M}, \mathcal{K}, \mathcal{E}, \gamma, \delta)$ be a p-information transmission system with $|M| > 2$. A *p-cryptanalyst* for $\mathfrak{I}$ is a triple $(\alpha_{\mathrm{p}}, \mu_{\mathrm{p}}, \upsilon_{\mathrm{p}})$ with $\mu_{\mathrm{p}} = p_E$ and

$$\upsilon_{\mathrm{p}} = \begin{cases} \lambda e, N. \left[\sum_{m \in N} 1 - |p_M(m) - p_{M|E}(m \mid e)|\right], & \text{if } p_E(e) > 0, \\ 0, & \text{if } p_E(e) = 0, \end{cases}$$

where, for $m \in M$ and $e \in E$, $p_{M|E}(m \mid e)$ is the probability of m given e.

With μ_{p} and υ_{p} as in Definition 4.2, one has $\mu_{\mathrm{p}}(\mathrm{dom}\alpha_{\mathrm{p}}) = 0$ if $p_E(e) = 0$ for all $e \in E$ with $\alpha_{\mathrm{p}}(e) \neq \emptyset$. Thus, cryptograms that could be cryptanalysed in principle – because of $\alpha_{\mathrm{p}}(e) \neq \emptyset$ – result from messages or keys which have probability 0. For $e \in E$ with $\alpha_{\mathrm{p}}(e) \neq \emptyset$ and $p_E(e) > 0$, consider

$$\upsilon_{\mathrm{p}}(e)(\alpha_{\mathrm{p}}(e)) = \sum_{m \in \alpha_{\mathrm{p}}(e)} 1 - |p_M(m) - p_{M|E}(m \mid e)|.$$

This value is derived from differences between the a priori and a posteriori probabilities of messages given the cryptogram e. It is equal to $|M|$ when $p_M(m)$ and $p_{M|E}(m \mid e)$ are equal for all $m \in M$. It is smaller than $|M|$ when $p_M(m)$ and $p_{M|E}(m \mid e)$ differ for some m. It is equal to 0 if and only if $\alpha_{\mathrm{p}}(e) = \emptyset$ or $p_E(e) = 0$. The case of $|M| \leq 2$ is excluded to avoid the possibility that $\upsilon_{\mathrm{p}}(e)(\alpha_{\mathrm{p}}(e))$ could be 0 with $\alpha_{\mathrm{p}}(e) \neq 0$ and $p_E(e) > 0$; this is merely a technical restriction.

Definition 4.3 A p-information transmission system $\mathfrak{I} = (\mathcal{M}, \mathcal{K}, \mathcal{E}, \gamma, \delta)$ is said to *achieve p-perfect secrecy* if, for the p-cryptanalyst $(\alpha_{\mathrm{p}}^{\mathrm{full}}, \mu_{\mathrm{p}}, \upsilon_{\mathrm{p}})$, one has $\upsilon_{\mathrm{p}}(e)(M) = |M|$ for all $e \in E$ with $p_E(e) \neq 0$.

Remark 4.1 *A finite p-information transmission system $(\mathcal{M}, \mathcal{K}, \mathcal{E}, \gamma, \delta)$ achieves p-perfect secrecy if and only if it achieves perfect secrecy in the sense of Shannon.*

Using Bayesian arguments,

$$p_{M|E}(m \mid e) = \frac{p_{M \times E}(m, e)}{p_E(e)}$$

assuming that $p_E(e) \neq 0$

$$= \frac{p_M(m) \cdot p_{E|M}(e \mid m)}{p_E(e)}$$

and

$$p_{E|M}(e \mid m) = \sum_{\substack{k \in K \\ \gamma(m,k) = e}} p_K(k)$$

assuming that $\mathcal{M}$ and $\mathcal{K}$ are independent.

We now consider a specific p-information transmission system that also plays a key rôle in Shannon's analysis:

Example 4.2 Modifying the system of Example 3.1, let us assume for the sake of simplification that all messages to be encoded have the same length n, that is $M = E = K = X^n$ where $X = \{0, 1\}$. Moreover, let $p_K(k) = 2^{-n}$ for all $k \in K$. For every message $m \in M$ and every cryptogram $e \in E$, there is exactly one key $k \in K$ such that $e = \gamma(m, k)$. Therefore, $p_{E|M}(e \mid m) = 2^{-n}$ and

$$p_{M \times E}(m, e) = p_M(m) \cdot p_{E|M}(e \mid m) = p_M(m) \cdot 2^{-n}.$$

Hence,

$$p_E(e) = \sum_{m \in M} p_{M \times E}(m, e) = 2^{-n}.$$

Therefore,

$$p_{M|E}(m \mid e) = \frac{p_{M \times E}(m, e)}{p_E(e)} = p_M(m).$$

As a consequence of Example 4.2, one obtains the following result, originally due to Shannon. This result is often referred to as a proof that the so-called *one-time pad*[12] achieves perfect secrecy.

Proposition 4.1 *Let $\mathfrak{I} = (\mathcal{M}, \mathcal{K}, \mathcal{E}, \gamma, \delta)$ be a p-information transmission system such that $M = K = E$ and $|K| < \aleph_0$. Moreover, assume that $\mathcal{M}$ and $\mathcal{K}$ are independent, $p_K(k) = \frac{1}{|K|}$ for all $k \in K$, γ and δ are total, and that for every $m \in M$ and every $e \in E$ there is a unique $k \in K$ with $e = \gamma(m, k)$. Then $\mathfrak{I}$ achieves p-perfect secrecy.*

The reasoning leading to Definition 4.3 relies on the interpretation of the difference between the a priori and a posteriori probabilities as expressing information the adversary has obtained by receiving the encoded message. Thus, if $p_M(m) = p_{M|E}(m \mid e)$, the adversary has received no information about m from getting e.

Let us consider this argument in greater detail. Suppose the cryptanalyst receives a cryptogram which, after some effort, is made readable and exhibits a message of extreme importance – say, a nuclear attack is planned on the country for the next morning at 8 o' clock sharp; or terrorists plan to poison the water supply of a city; or a financial manager informs his confidents about the strategy to use for playing out one currency against another one –; suppose the cryptananlyst also knows that a system like the above has been used to achieve perfect secrecy. Would the cryptanalyst discard the result of his analysis? Would he really say that any message could have resulted in that cryptogram and that he did not learn anything – because the probabilities did not change – and that, therefore, the result of his cryptanalysis was wrong or meaningless? Or would he not rather conclude that the sender used a *weak* key?

---

[12] As mentioned in Section 1, the literature uses two kinds of arguments for the unbreakability of the one-time pad. The second approach is analysed in Section 7 below.

One might argue that the cryptanalyst should assume that sender and recipient would use the system "properly," that is, avoid using weak keys.[13] But, what is a weak key? Beyond the operational definition – a key is weak if messages encrypted with it can be cryptanalysed (easily) – there is no definition of a weak key; there is definitely no mathematically satisfactory definition of a weak key. So, how is the sender to know whether a key to be used is weak? This is just a variant of the general dilemma of cryptography: sender and recipient believe their communication to be secret, while the cryptanalyst is eagerly reading it and not telling them about their vulnerabilities. In other words,

- *the definition of p-perfect secrecy, Definition 4.3, permits proving systems p-perfectly secret which have weak keys without providing a means to determine, a priori, which keys are weak.*

Moreover, even if we do accept that sender and recipient use the system properly, that is, that the dramatic reading found of the cryptogram is indeed as likely or unlikely as any other reading, because its probability did not change, does not the contents of the reading render it too risky to discard? This suggests that

- *risk rather than probability might be an appropriate measure of secrecy.*

Concretely, consider the cryptographic system of Example 4.2. Let $i \in \mathbb{N}$ be large. Clearly, there are many keys $k \in X^i$ such that, for many or even all messages $m \in M_i$, the cryptogram $k \oplus m$ nearly gives away the message. If the sender happens to choose the key $k = 00 \cdots 0$ for example, then $k \oplus m = m$. Should the cryptanalyst discard this?[14] And yet, the system achieves perfect secrecy according to Definition 4.3!

The *cryptanalyst's dilemma* can be explained as follows: While it may be extremely unlikely that a weak key has been used, he cannot ignore the result of his cryptanalysis if the consequences of doing so are disastrous. Hence,

- *the probability of successful cryptanalysis is insufficient as a cost measure when assessing secrecy.*

In this respect, the situation in cryptography is not different from that in risk analysis in other areas: One has to assess the expected cost,[15] not the probability. Moreover, the definition of perfect secrecy does not take into account that a cryptographic system may not be uniformly strong across all messages and keys. Hence,

- *local weaknesses – weak keys – need to be taken into account.*

---

[13] Ironically, if the sender avoids weak keys then the resulting system cannot be *proven* to achieve p-perfect secrecy, that is, perfect secrecy in the sense of Shannon any more. This is shown in Section 7 below.

[14] Of course there can be all kinds of additional psychological tactics that add another layer of confusion; but the underlying results remain the same.

[15] We use the word *expected* in the colloquial, not in the mathematical sense here. The difficulty stems from the interpretation of small probabilities and of probability 0. Because of its small probability the cost of disastrous event – like a nuclear accident – may not contribute much to the expected cost (in the mathematical sense); it may, however, be too high a price at all to let that event ever happen. This analogy should indicate that improbability alone is not sufficient to assess secrecy.

The notion of *weak key* has, however, no rigorous definition in the cryptographic literature.

In the choice of υ_{p} in Definition 4.2, a specific method of comparing probability distributions was chosen. Many other methods would serve the same purpose, that is could be used instead of the expression

$$p_M(m) - p_{M|E}(m \mid e)$$

in the definition of υ_{p}. A natural alternative is the *divergence*

$$p_M(m) \log \frac{p_M(m)}{p_{M|E}(m \mid e)}.$$

Some details of the arguments change, but the essence remains the same, that is, systems which are breakable can be proven to provide perfect secrecy in the strict sense of the definition.

The information transmission system of Example 4.2 is often used to show, via Proposition 4.1, that the one-time pad, usually equated to the Vernam cipher, achieves perfect secrecy (for example [38]; [35], pp. 535–537; [18], pp. 22–23; [39], pp. 48–51). In the sequel we refer to this version of the one-time pad as the *p-one-time pad.* As mentioned in Section 1, there is another kind intuition about the one-time pad in the literature, to be called the *r-one-time pad;* that version is analysed in greater detail in Section 7 below. While not achieving perfect secrecy in the sense of Shannon it seems to be much closer to achieving true perfect secrecy. Combining Example 4.2 and Proposition 4.1, we obtain the following observation.

Corollary 4.1 *The p-one-time pad achieves p-perfect secrecy; hence, it achieves perfect secrecy in the sense of Shannon.*

5. Information Theoretic Aspects

In this section we formulate Shannon's unicity distance arguments ([38], [23], [28]) in our general framework.

Definition 5.1 Let $\mathfrak{I} = (\mathcal{M}, \mathcal{K}, \mathcal{E}, \gamma, \delta)$ be a p-information transmission system. An *i-cryptanalyst* for $\mathfrak{I}$ is a triple $(\alpha_{\mathrm{p}}, \mu_{\mathrm{i}}, \upsilon_{\mathrm{i}})$ with $\mu_{\mathrm{i}} = p_E$ and

$$\upsilon_{\mathrm{i}} = \begin{cases} \lambda e, N.[1 + H_{M|e}(N \mid e)], & \text{if } N \neq \emptyset \text{ and } p_E(e) > 0, \\ 0, & \text{if } N = \emptyset \text{ or } p_E(e) = 0, \end{cases}$$

where, for $N \subseteq M$ and $e \in E$ with $p_E(e) > 0$,

$$H_{M|e}(N \mid e) = - \sum_{m \in N} p(m \mid e) \log p(m \mid e).$$

In interpreting the unicity measure $\upsilon_{\mathrm{i}}(e)(\alpha_{\mathrm{p}}(e))$ of an i-cryptanalyst we have to distinguish three cases as before: When $\upsilon_{\mathrm{i}}(e)(\alpha_{\mathrm{p}}(e)) = 0$ then $\alpha_{\mathrm{p}}(e) = 0$ or $p_E(e) = 0$. Otherwise, $\upsilon_{\mathrm{i}}(e)(\alpha_{\mathrm{p}}(e))$ is at least 1. In this case, $\upsilon_{\mathrm{i}}(e)(\alpha_{\mathrm{p}}(e)) - 1$ measures the amount of uncertainty about the messages in $\alpha_{\mathrm{p}}(e)$ when the cryptogram e has been received by the adversary. If the value of $\upsilon_{\mathrm{i}}(e)(\alpha_{\mathrm{p}}(e))-1$ is small then it is likely that the cryptogram e received by the i-cryptanalyst corresponds to only very few messages in $\alpha_{\mathrm{p}}(e)$ with high enough probability. With this interpretation, the following definition is quite natural.

Definition 5.2 A p-information system $\mathfrak{I} = (\mathcal{M}, \mathcal{K}, \mathcal{E}, \gamma, \delta)$ achieves *i-perfect secrecy* if, for the i-cryptanalyst $(\alpha_{\mathrm{p}}^{\mathrm{full}}, \mu_{\mathrm{i}}, \upsilon_{\mathrm{i}})$, one has

$$\upsilon_{\mathrm{i}}(e)(M) = 1 + H_{M|e}(M \mid e)$$

for all $e \in E$ with $p_E(e) > 0$.

The proof of Proposition 4.1, indicated in Example 4.2, can also be used to prove the following result.

Proposition 5.1 *Let $\mathfrak{I} = (\mathcal{M}, \mathcal{K}, \mathcal{E}, \gamma, \delta)$ be a p-information transmission system such that $M = K = E$ and $|K| < \aleph_0$. Moreover, assume that $\mathcal{M}$ and $\mathcal{K}$ are independent, $p_K(k) = \frac{1}{|K|}$ for all $k \in K$, γ and δ are total, and that for every $m \in M$ and every $e \in E$ there is a unique $k \in K$ with $e = \gamma(m, k)$. Then $\mathfrak{I}$ achieves i-perfect secrecy.*

This implies that the i-cryptanalyst is in exactly the same dilemma as the p-cryptanalyst. What is he or she to do with a readable cryptogram knowing the system achieves i-perfect secrecy?

Instead of measuring secrecy in terms of μ_{i} and υ_{i}, Shannon [38] proposed to measure the overall secrecy achieved by a p-information transmission system in terms of the message equivocation (or key equivocation) given an arbitrary cryptogram. This measure, expressed in our framework, leads to the following definition.

Definition 5.3 Let $\mathfrak{I} = (\mathcal{M}, \mathcal{K}, \mathcal{E}, \gamma, \delta)$ be a p-information transmission system. A *u-cryptanalyst* for $\mathfrak{I}$ is a triple $(\alpha_{\mathrm{p}}, \mu_{\mathrm{u}}, \upsilon_{\mathrm{u}})$ with $\mu_{\mathrm{u}} = p_E$ and

$$\upsilon_{\mathrm{u}} = \begin{cases} \lambda e, N.[1 + H_{M|E}(N \mid E)], & \text{if } N \neq \emptyset, \\ 0, & \text{if } N = \emptyset, \end{cases}$$

where, for $N \subseteq M$ and $e \in E$,

$$H_{M|E}(N \mid E) = \sum_{e \in E} p_E(e) \sum_{m \in N} -p(m \mid e) \log p(m \mid e).$$

Then *u-perfect secrecy* would be achieved when

$$\upsilon_{\mathrm{u}}(e)(M) = 1 + H_{M|E}(M \mid E) = 1 + H_M(M).$$

Note that $\upsilon_{\mathrm{u}}(e)(M) - 1 = H_{M|E}(M \mid E)$ is the message equivocation given an arbitrary cryptogram and, of course, does not depend on e at all. When this value is close to zero then, with high probability, the cryptanalyst will only have few possible messages associated with each cryptogram. As emphasized in [25] and [28], *message equivocation,* being an expectation, can only be used to measure lack of secrecy.

The unicity measures υ_{i} and υ_{u} reveal an important point – observed already by Shannon and probably even earlier. Cryptographic secrecy has three aspects:

(1) A cryptogram may not be cryptanalysable in principle. This is captured in our α_{p} and μ.

(2) A cryptogram may be cryptanalysable, but lead to a large number of essentially different messages. We capture this case by υ being large.

(3) A cryptogram may be cryptanalysable and lead to a small number of inessentially different messages; this is captured by υ_{i} being small.

Cases (1) and (2) have been adressed so far and will be re-visited in Section 7. Case (3), is considered in the next section.

6. Cryptography and Computational Complexity

In this section we consider the situation when, according to the unicity measure, a given information transmission system is weak. This means that, whenever $\alpha_{\mathrm{p}}(e) \neq \emptyset$ then $\alpha_{\mathrm{p}}(e)$ may be small and, therefore, the cryptanalyst would usually be quite certain about the original message. In this situation, one would have to rely on the access measure μ to provide the required secrecy. This means that the set

$$\{e \mid \alpha_{\mathrm{p}}(e) \neq \emptyset\}$$

should be made small.

In this section, we assume that M, K, and E are represented over some fixed alphabet. Moreover, we assume that M and K are recursively enumerable and that γ and δ are partial recursive functions. Then also E and $\alpha_{\mathrm{p}}^{\mathrm{full}}$ are recursively enumerable. Knowing the information transmission system in use, an adversary can, therefore, always obtain $\alpha_{\mathrm{p}}^{\mathrm{full}}$ – at least in principle. With the probabilities given in a suitable constructive fashion, the cryptanalyst can also compute the access and unicity measures of a p-information system. However, this precomputation of all cryptogram-message pairs is extremely expensive computationally. Hence a concrete passive access potential α_{p} will reflect the adversary's cost limitations – limitations of computational resources, required timeliness of cryptanalysis and so on; hence, such an α_{p} will usually be much smaller than $\alpha_{\mathrm{p}}^{\mathrm{full}}$.

In [27], the security of cryptographic systems is explored from the point of view of computational complexity, using the settings of the theory of recursive functions and of Blum's theory of complexity measures.[16] The security of a cryptographic system is measured there by three partial recursive functions – χ, η, and χ'; χ is an upper bound on the complexity of encryption and decryption; η

[16] For a general introduction to recursive functions including Blum's complexity theory see [10]. Blum's complexity theory was first published in [7]. An analysis of cryptography using *general* complexity theoretic considerations is also given in [9].

is an upper bound on the complexity of cryptanalysis; χ' is an uppper bound on the complexity of decryption by the cryptanalyst after cryptanalysis.[17] Under some natural assumptions one can show that η and χ' need not be more than exponentially larger than χ – this has been observed for the usual cases also in [9] and elsewhere and corresponds to the availability of the *brute-force attack,* that is, the attack of trying all possibilities. Moreover, the predicate of *a given cryptographic system being* (χ, η, χ')*-secure* is in the class Π_4 of the arithmetic hierarchy and may even be Π_4-complete.[18]

Since providing the technical details would require too much space, we only outline the application of computational complexity theory in our general framework and appeal to the intuition of the reader. For a given pair of partial recursive functions (η, χ') we define $\alpha_{\mathrm{p}}^{\eta,\chi'}$ to be the set of pairs $(m \mid e) \in \alpha_{\mathrm{p}}^{\mathrm{full}}$ such that the cryptanalyst's cost[19] for cryptanalysing e does not exceed $\eta(e)$, the result of the cryptanalysis yields a correct decryption algorithm φ' such that $\varphi'(e) = m$ and the cost of applying φ' to e does not exceed $\chi'(e)$. Thus, $\alpha_{\mathrm{p}}^{\eta,\chi'}$ is the set of all pairs $(m \mid e) \in \alpha_{\mathrm{p}}^{\mathrm{full}}$ such that cryptanalysis is easy and leads to m – when measured by η and χ'.

Definition 6.1 Let $\Im = (M, K, E, \gamma, \delta)$ be an information transmission system such that M, K, and E are recursively enumerable represented sets and such that γ and δ are partial recursive functions. Then $\Im$ is said to be a *computable information transmission system.*

Definition 6.2 Let $\Im = (M, K, E, \gamma, \delta)$ be a computable information transmission system and let η and χ' be partial recursive functions[20]. An (η, χ')*-c-cryptanalyst* for $\Im$ is a cryptanalyst $(\alpha_{\mathrm{p}}^{\eta,\chi'}, \mu, \upsilon)$.

In Definition 6.2, the parameters μ and υ can still be chosen freely: In particular, one could choose these based on cardinality or probability.

---

[17] This model takes into account that the legitimate users of the information transmission system and the adversary may have vastly different computational resources.

[18] It is definitely not in a class lower than Σ_2, [27].

[19] Except in examples we have, so far, made no assumptions about the actual representation of messages, keys, and cryptograms. For recursion theoretic and complexity theoretic arguments, we have to fix a representation, for example that by strings (finite or infinite) over some alphabets. This is assumed in the sequel. Moreover, we assume that a cryptanalysis leads to an algorithm by which all cryptograms encoded using the same key can be decrypted. This is the definition used in [27], and it is in agreement with the intuition expressed in the cryptographic literature. Strictly speaking, using the arguments of Section 4, this intuition is risky. In the case of a very important message, as an adversary, one does not care at all whether one could also decrypt all other cryptograms resulting from using the same or an equivalent key. Further to this problem see [27].

[20] Once again, we appeal to the readers' intuition to fill in the details about domains and co-domains of these functions. These can be found in [27].

Definition 6.3 Let $\mathfrak{I} = (M, K, E, \gamma, \delta)$ be a computable information transmission system, let χ, η, and χ' be partial recursive functions, and let μ be a passive access measure for $\mathfrak{I}$. Then $\mathfrak{I}$ is said to achieve (χ, η, χ')-*c-perfect secrecy* with respect to μ if the following conditions are satisfied:

(1) There are algorithms for γ and δ the complexity of which is bounded by χ.
(2) $\mu(\{e \mid \alpha_{\mathrm{p}}^{\eta,\chi'}(e) = \emptyset\}) = 0$.

In Definition 6.3, condition (2) may have vastly different meanings. If μ is the cardinality then that condition implies that no cryptogram can be cryptanalysed within the given resource constraints; when μ is probability then this is true only with probability 1. Thus, μ serves as an additional parameter by which to express the degree of secrecy.

Basing the definition of *perfect secrecy* on complexity theory requires a relativization – with respect to the cost for authorized encryption and decryption, for cryptanalysis, and for unauthorized decryption. This relativization itself is quite acceptable in principle. However, even granted this setting, there may be no acceptable definition of perfect secrecy, for various reasons:

- Even relativized perfect secrecy is *highly* undecidable in general.
- Proofs of relativized perfect secrecy are extremely difficult [9].
- Complexity bounds apply to *almost all cases* only.

These points seem to indicate that computational complexity may not be the right setting either in which to attempt a definition of *perfect secrecy.*

The last of these points, that complexity bounds are almost-always bounds only, introduces a technical mathematical problem and, as is well known, a cryptographic problem.

7. Cryptography and Program-Size Complexity

We have seen, so far, that according to the probabilistic definition of perfect secrecy, p-perfect secrecy, systems which have weak keys can be proven perfectly secret. The approaches using information theory or computational complexity, i-perfect or c-perfect secrecy, have similar deficiencies. To explore this issue further, we return to the single example of a cryptographic system universally believed to achieve intuitive perfect secrecy, the one-time pad.

In the cryptographic literature, the arguments for the strength of the one-time pad come in two variants which are sometimes even mixed. First, there is the p-one-time pad as introduced in Section 4. In this case, one has a system achieving p-perfect secrecy, that is, perfect secrecy in the sense of Shannon, but permitting weak keys. Second, a system is considered in which the keys are random strings and it is argued that the cryptograms will be random strings too, assuming that the messages are non-random ([37], p. 14, for example; implicitly also [34], p. 342); in this case, there will be no possibility of cryptanalytic attack. Note that in the second case the weak keys seem to have been eliminated.

We have already discussed the first approach. In this section we consider the second one. We do believe that, in essence, the arguments used to support the strength of the one-time pad in the second sense are intuitively valid. We show, however, that they are not correct mathematically. Moreover, we show that a one-time pad of the second kind does not achieve p-perfect secrecy, that is, does not achieve perfect secrecy in the sense of Shannon. As mentioned before, this does not mean that the one-time pad is bad – in particular the one of the second kind –, but that the definition of p-perfect secrecy does not capture the intuitive notion of perfect secrecy or unbreakability. We discuss the consequences of these findings in Section 8 below.

To make our presentation precise, we introduce some basic terminology from the theories of program-size complexity and algorithmic information (see [11] or [33]).

Let X be an alphabet with $|X| > 1$ and let φ be a partial recursive function of X^* into X^* such that, for $u, v \in X^*$, if φ is defined on both u and uv then v has length 0. For $u \in X^*$, let $H_\varphi(u) = \min\left\{|v| \,\middle|\, v \in X^*, \varphi(v) = u\right\}$ with $H_\varphi(u) = \infty$ if there is no v with $\varphi(v) = u$. $H_\varphi(u)$ is the *φ-program-size complexity* of u. The φ-program-size complexity[21] does not really depend on φ in the following sense: There is a partial recursive function ψ such that, for every φ, there is a constant $c_{\psi,\varphi}$ satisfying $H_\psi(u) \leq H_\varphi(u) + c_{\psi,\varphi}$ for all $u \in \mathrm{dom}\varphi$. In the sequel, let ψ be an arbitrary but fixed function with this property and we write H instead of H_ψ. For $u \in X^*$, $H(u)$ is called the *program-size complexity*[22] of u.

For $n \in \mathbb{N}$, let

$$\Sigma(n) = \max_{u \in X^n} H(u).$$

Thus, $\Sigma(n)$ is the maximal program size required to compute a string of length n. One can show that $\Sigma(n)$ is equal to $n + H(\mathrm{str}(n))$ up to an additive constant, where $\mathrm{str}(n)$ is the nth string with respect to the quasi-lexicographic order on X^*.

Definition 7.1 Let $t \in \mathbb{N}_0$. A finite string $u \in X^*$ is said to be *t-random* if $H(u) \geq \Sigma(|u|) - t$. The string u is *random* if it is t-random for $t = 0$.

Many definitions of randomness of strings in X^∞ exist in the literature (see [11] or [33]). For *finite* strings, Definition 7.1, is the most convenient one in our context and, one could argue, the most adequate one in general [12].

The set of random strings of length n is non-empty for all n. More precisely, there is a constant $c \in \mathbb{N}$ such that

$$|\{u \mid u \in X^n, H(u) = \Sigma(n)\}| > |X|^{n-c}$$

for all $n \in \mathbb{N}$. On the other hand, for *n large enough,* there are also non-random strings of length n; the strings 0^n, 1^n, $(01)^n$ are such examples.

Typically, one assumes that messages are of comparatively low complexity – at least non-random. To some extent, this corresponds to Shannon's assump-

---

[21] The definition we use is due to Chaitin [16]; see [11]. Alternative definitions due to Kolmogorov [31] and others are less simple to use for our purposes.

[22] Note that, traditionally, program-size complexity is denoted by the symbol H – as is information; the particular meaning of H should be clear from the context.

tions about the stochastic properties of the message source (see [38] and [28] for details).[23]

On the other hand, it is a commonly accepted view that in a cryptographic system, to achieve a certain degree of secrecy, the cryptograms have to appear to be random strings – without any regularities or patterns that would permit the adversary to launch an attack with statistical methods (for example [34], p. 342; [8], p. 17; [2], p. 246; [3], p. 148; [19]; [14]). This intuition leads to the following variant of the one-time pad.

Definition 7.2 Let K be the set of finite random strings over $X = \mathbb{B}$, let M be the set of finite non-random strings over X, let γ and δ be the componentwise exclusive or operation, and let $E = \gamma(M, K)$. The information transmission system $(M, K, E, \gamma, \delta)$ is called the *r-one-time pad.*

The definitions of p-one-time pad and r-one-time pad can be generalized to the non-binary case and to infinite strings in the obvious fashion – in the spirit of Vernam's original definition.[24]

We now show that the r-one-time pad does not achieve perfect secrecy in the sense of Shannon. For this purpose, we need to consider probabilities on M and K. We fix n and consider only messages, keys, and cryptograms of length n. Thus, let $M_n = M \cap X^n$, $K_n = K \cap X^n$, and $E_n = E \cap X^n$. We require, that all messages of length n have a strictly positive probability and that all keys of that length are equally likely. The former means that $p_{M_n}(m) > 0$ for all $m \in \mathbb{M}_n$. The latter is expressed by $p_{K_n}(k) = |K_n|^{-1}$ for all $k \in K_n$. For large enough n the sets M_n and K_n are non-empty and, therefore, these assumptions are possible.

Proposition 7.1 *For $n \in \mathbb{N}$, let $\mathfrak{I}_n = (\mathcal{M}_n, \mathcal{K}_n, \mathcal{E}_n, \gamma, \delta)$ be a p-information system such that $p_{M_n}(m) > 0$ for all $m \in M_n$ and $p_{K_n}(k) = |K_n|^{-1}$ for all $k \in K_n$. Moreover, with*

$$M = \bigcup_{n\in\mathbb{N}} M_n, \quad K = \bigcup_{n\in\mathbb{N}} K_n, \quad \textit{and} \quad E = \bigcup_{n\in\mathbb{N}} E_n,$$

assume that $(M, K, E, \gamma, \delta)$ is the r-one-time pad. For almost all n, the system $\mathfrak{I}_n$ does not achieve perfect secrecy in the sense of Shannon.

---

[23] This assumption is also made in [37], p. 14, for example.

[24] The history of the invention of the Vernam cipher is rather complicated. It seems that one of the crucial ideas, to use a key of a length comparable to the length of the message, was already around in 1914; its realization, to use a random key and to use it only once, and its implementation on a machine were proposed by Mauborgne and Vernam no later than 1917. A description of the system was first published in 1926 [40]. A similar system, for manual encryption, was invented in Germany by Kuntze, Schauffler, and Langlotz no later than 1921. For details see [29], pp. 397–403 and 1043–1045; [1], pp. 109–111.

Proof: Assume n is large. We first show that, for every $e \in E_n = \gamma(M_n, K_n)$, there is an $m \in M_n$ such that, for all $k \in K_n$, $\gamma(m,k) \neq e$. Indeed, if e is non-random then let $m = e$. This implies that $k = 0^n$, hence $k \notin K_n$ if n is large enough. On the other hand, if e is random, $e = e_1e_2e_3\cdots$ with $e_i \in X$ for all $i \in \mathbb{N}$, let $m = e_1 0 e_3 0 e_5 0 \cdots$; then $m \in M_n$, but $k = 0 e_2 0 e_4 0 e_6 0 \cdots$ and again $k \notin K_n$ if n is large.

Now consider $e \in E_n$. Then

$$0 < p_{E_n}(e) = \sum_{m \in M_n} \sum_{\substack{k \in K_n \\ m \oplus k = e}} p_{M_n}(m) \cdot |K_n|^{-1} < |K_n|^{-1}.$$

Let $m \in M_n$. Then

$$p_{E_n|M_n}(e \mid m) = \begin{cases} 0, & \text{if } e \oplus m \notin K_n, \\ |K_n|^{-1}, & \text{otherwise.} \end{cases}$$

Hence

$$p_{M|E}(m \mid e) = \begin{cases} 0 < p_{M_n}(m), & \text{if } e \oplus m \notin K_n, \\ \dfrac{|K_n|^{-1} \cdot p_{M_n}(m)}{p_{E_n}(e)} > p_{M_n}(m), & \text{otherwise.} \end{cases}$$

□

The crucial point in the proof of Proposition 7.1 is that there is a cryptogram e and a message m such that $e \oplus m$ is not a key.. Thus, a result similar to Proposition 7.1 can be proved under the much weaker assumption that there exist $e \in E_n$ and $m \in M_n$ such that $e \oplus m \notin K_n$. In Proposition 7.1, for *every* long enough message m and cryptogram e, one has $p(m) \neq p(m \mid e)$. A bound on the length n for which $\mathfrak{I}_n$ does not achieve perfect secrecy in the sense of Shannon can be inferred from the proof. The strings 0^n and $e_1 0 e_3 0 e_5 0 \cdots$ and similar ones must be non-random. This implies that n does not have to be extremely large.

The statement of Proposition 7.1 is counter-intuitive. Removing weak keys from the p-one-time pad, a common cryptographic practice to strengthen the system cryptographically, weakens the system in terms of Shannon's theory. If the cryptographic practice is right – and we certainly believe that – then the definition of perfect secrecy in the sense of Shannon, p-perfect secrecy, does not model what it claims to model.

Definition 7.3 Let $\mathfrak{I} = (M, K, E, \gamma, \delta)$ be a computable information transmission system. An r-cryptanalyst for $\mathfrak{I}$ is a cryptanalyst $(\alpha_{\mathrm{p}}, \mu, \upsilon)$ such that $\alpha_{\mathrm{p}} \subseteq \alpha_{\mathrm{p}}^{\mathrm{r}} \in A_{\mathrm{p}}(\mathfrak{I})$ where

$$\alpha_{\mathrm{p}}^{\mathrm{r}} = \left\{ (m \mid e) \,\middle|\, (m \mid e) \in \alpha_{\mathrm{p}}^{\mathrm{full}}, e \text{ is non-random} \right\}.$$

Thus, for the r-cryptanalyst, only cryptograms which are non-random strings may permit access to the corresponding messages. Probability and cardinality are obvious candidates for μ and υ; however, other outer measures can also be used.

We now turn to the definition of r-perfect secrecy.

Definition 7.4 Let $\mathfrak{I} = (M, K, E, \gamma, \delta)$ be a computable information transmission system and let μ be an access measure. Then $\mathfrak{I}$ is said to achieve *r-perfect secrecy* with respect to μ if $\mu(\mathrm{dom}\alpha_{\mathrm{p}}^{\mathrm{r}}) = 0$.

According to a quite common belief, if $\mathfrak{I} = (M, K, E, \gamma, \delta)$ is an r-one-time pad, then $\gamma(m, k)$ is a random string – or at least a pseudo-random string – for $m \in M$ and $k \in K$ (for example [37], pp. 13–14; [21], p 172; [20], p. 182; [2], pp. 243–246; [5], pp. 20–21; [3], p. 166; [32], p. 116). If every cryptogram is a random string, it would follow that the r-one-time pad achieves r-perfect secrecy with respect to $\mu_{|\,\cdot\,|}$. We prove that this is not true, that is, the r-one-time pad has cryptograms which are non-random and even not pseudo-random.

Our next result states a lower bound on the program-size complexity of cryptograms obtained from one-time pad-like information transmission systems.

Proposition 7.2 *Let $f : X \times X \to X$ be a (recursive) function such that $\lambda w.[f(x, w)]$ is injective for all $x \in X$ and extend f, componentwise, to a mapping of $X^* \times X^*$ into X^*. Let $k, m \in X^*$ such that $H(m) \leq H(k) + c$ for some constant c and all $i \in \mathbb{N}$. Then*

$$H(f(m, k)) \geq H(k) - H(m) + c'$$

for some constant c' and all i.

Proof: Given $f(m, k)$ and m, one can determine k uniquely. Therefore,

$$H(k) \leq H(f(m, k)) + H(m) - c'$$

for some constant c'. □

For $X = \mathbb{B}$, the operation $\oplus$ satisfies the assumptions about f in Proposition 7.2. Thus, if k is interpreted as the key, m as the message, and $m \oplus k$ as the cryptogram, then the complexity of the cryptogram is bounded from below – only – by the complexity of the key minus the complexity of the message. The following example shows that this bound is tight, that is, in an extreme situation the program-size complexity $H(m \oplus k)$ can be nearly as low as $H(k) - H(m)$.

Example 7.1 Let $X = \{0, 1, \ldots, q - 1\}$ with $q > 1$ and let $n \in \mathbb{N}$. We assume that n is large, greater than 1000, say. Let $u \in X^n$ be random, and let $v \in X^n$ be such that

$$v_i = \begin{cases} -u_i \pmod{n}, & \text{if } i \text{ is even,} \\ 0, & \text{if } i \text{ is odd,} \end{cases}$$

for $i = 1, 2, \ldots, n$ where $u = u_1 u_2 \cdots u_n$ and $v = v_1 v_2 \cdots v_n$ with $u_i, v_i \in X$. Then $H(u) = \Sigma(n)$ and $H(v) \leq \Sigma\left(\frac{n}{2}\right) + c_v$ for some constant c_v. Thus, v is non-random. Now

$$v_i \oplus u_i = \begin{cases} 0, & \text{if } i \text{ is even,} \\ u_i, & \text{if } i \text{ is odd,} \end{cases}$$

and, therefore, $H(u \oplus v) \leq \Sigma\left(\frac{n}{2}\right) + c$ for some constant c.

The example shows not only that the bound of Proposition 7.2 is tight, but also, that the componentwise combination of a random and a non-random sequence need not be random, not even pseudo-random, at all; and this happens even with such a simple function as the exclusive or for the binary alphabet.

Proposition 7.3 *Let μ be an access measure for the r-one-time pad. If μ is such that $\mu(E') = 0$ implies $E' = \emptyset$ for $E' \subseteq E$, then the r-one-time pad does not achieve r-perfect secrecy with respect to μ.*

Proof: As shown in Example 7.1, $\mathrm{dom}\alpha_{\mathrm{p}}^{\mathrm{r}} \neq \emptyset$. By the assumption about μ, $\mu(\mathrm{dom}\alpha_{\mathrm{p}}^{\mathrm{r}}) > 0$. □

Thus, the second common argument used to show that the one-time pad achieves perfect secrecy is mathematically incorrect. Of course, our counter-example is rather artificial; the message is random in every second position.

Proposition 7.3, relies on the assumption that $\mu(E') = 0$ implies $E' = \emptyset$. This assumtion is satisfied by $\mu_{|\,.\,|}$, that is cardinality. If we use the probability p_E instead, then $\mu(\mathrm{dom}\alpha_{\mathrm{p}}^{\mathrm{r}}) = 0$ only means that non-random cryptograms appear with probability 0. We believe this could be possible to achieve in the limit as $n \to \infty$. However, in this case, the arguments made earlier when discussing p-perfect secrecy and the p-one-time pad apply again.

As a consequence of Proposition 7.2 one can indeed find an information transmission system that nearly achieves r-perfect secrecy as follows.

Proposition 7.4 *Let $c \in \mathbb{N}$ be an arbitrary, but fixed constant, and let $X = \mathbb{B}$. For $n \in \mathbb{N}$, let K_n be the set of random strings over X, and let*

$$M_n = \{u \mid u \in X^n, H(u) \leq c\}.$$

Let

$$K = \bigcup_{n \geq N} K_n \text{ and } M = \bigcup_{n \geq N} M_n,$$

and let

$$\mathfrak{I} = (M, K, E, \gamma, \delta)$$

be the information transmission system with γ and δ the componentwise exclusive or and $E = \gamma(M, K)$. Then every $e \in \mathrm{dom}\alpha_{\mathrm{p}}^{\mathrm{r}}$ is c-random.

Proof: Consider $m \in M_n$ and $k \in K_n$. By Proposition 7.2,

$$H(m \oplus k) \geq \Sigma(n) - H(m) \geq \Sigma(n) - c$$

using the assumption that $H(m) \leq c$ and the fact that $H(m) \leq \Sigma(n) = H(k)$. This holds true for any $n \in \mathbb{N}$. □

The restriction in Proposition 7.4 – that $H(m) \leq c$ for all $m \in M$ – is severe: It says that *all messages in the system* can be computed using programs that are no longer than c bits. Moreover, c should be small for the system to achieve the promised degree of secrecy in a practically relevant way; in particular, c needs to be small if secrecy is to be afforded for values of n which are realistically small.

Such a bound on c could imply, however, that the message space M becomes unusably small.

There is, however, another potential problem with the concept of r-perfect secrecy or that of c-r-perfect secrecy suggested by Proposition 7.4: For every constant $c \in \mathbb{N}_0$ and every $v \in X^*$ there exist $u, w \in X^*$ such that uvw is c-random (see [11], Theorem 5.47). This is not surprising at all; it but indicates that the definition of the r-one-time pad, Definition 7.2, still permits the presence of keys that contain long cryptographically weak substrings. Moreover, these are by no means rare, but appear with a relative frequency which is very close to their a priori probability.[25] Thus, as in the case of the p-one-time pad, the r-one-time pad itself cannot, in principle, rule out that keys with theoretical weaknesses are used.

8. Conclusions

A mathematical definition $\mathbb{S}$ of *perfect secrecy* must satisfy at least the following two conditions:

(1) If a system $\mathfrak{I}$ can be proven to achieve perfect secrecy according to $\mathbb{S}$, then it has no cryptographic weakness.

(2) If a system $\mathfrak{I}$ is cryptographically unbreakable then it can be proven to achieve perfect secrecy according to $\mathbb{S}$.

By these standards, the notion of p-perfect secrecy fails condition (1); if one accepts that the r-one-time pad achieves perfect secrecy – and no reason has been given to doubt this – then the notion of r-perfect secrecy fails condition (2).

For a definition $\mathbb{S}$ of perfect secrecy, failing to satisfy condition (1) is more serious than failing to satisfy condition (2); in the former case, a system with cryptographic weakness may be classified as being highly secure, in fact unbreakable; in the latter, a truly unbreakable system may just not be provably unbreakable.

The evidence accumulated in this paper seems to indicate that, so far, there is no mathematically rigorous definition of perfect secrecy which would satisfy the conditions listed above. We have exposed the shortcomings of four natural candidates for such a definition using vastly different approaches, based on ideas drawn from probability theory, information theory, the theory of computational complexity, and the theory of program-size complexity.

There seem to be only three fundamental issues that cause these difficulties:

(1) The presence of weak keys and the lack of a rigorous definition of the notion of *weak key*.

(2) The absence of a representation of risk to compensate for an otherwise too optimistic assessment based on low probabilities or on probabilities which are 0.

(3) The fact that complexity theoretic statements usually hold only for *almost all* ...

---

[25] For a detailed analysis, see [11], Chapter 5.6.

It has been argued that avoidance of weak keys should be treated as a key management issue which has nothing to do with the cryptographic system itself. We disagree. Perfect secrecy is meant to be a predicate asserting the cryptographic strength of a system, and that assessment should take into account which keys are actually used and how they are actually used. Otherwise, the key management may completely spoil the achievable degree of secrecy. Indeed, when the weak keys are eliminated from the one-time pad, the resulting system no longer achieves perfect secrecy (Proposition 7.1). One could argue that we have eliminated too many or too few or the wrong kind of keys; however, the loss of perfect secrecy is just a consequence of the fact that *some* keys have been eliminated – and a single one would have been sufficient. On the other hand, the removal of weak keys seems to strengthen the system's achievable secrecy, an assessment that – it seems – cannot be expressed using Shannon's definition of secrecy.

In fact, Proposition 7.1 suggests that, rather than treat the weak keys as a key management issue, one ought to deal with weak keys in the evalution of the cryptographic system itself. There is no rigorous definition of the notion of *weak key.* We have shown that using only random strings as keys – as is often suggested in the literature for the one-time pad – does not achieve the secrecy claimed and, moreover, does not rule out the presence of weak parts in keys.

It seems, a definition of the notion of *weak key* may have to be formulated in conjunction with that of *secrecy,* both based on the intuitive operational concepts these notions convey.

One can also argue that events which lead to insecurities – usage of weak keys – occur with such a small probability that, by all practical standards, the possibility of these events can be ignored. This is probably true when little is at stake. If, however, unauthorized information access can lead to truly vast damage – say, the crash of the world's financial system or loss of life – then the assessment cannot be purely based on probability. These considerations suggest that a mathematical model of secrecy also needs to take risk factors into account.

It may well be that a definition of *perfect secrecy* satisfying the two conditions listed at the beginning of this section is impossible. It may also be, that for any such definition there is no cryptographic system achieving perfect secrecy. It seems that the approach to take now is to replace the notions of perfect secrecy and weak key by formal notions of *level of secrecy* and *level of weakness of a key.*

Finally, in the literature one frequently finds the argument that, for a cryptogram to offer no point of attack, the cryptogram should be or look random. In the sense that a random string would offer no point of attack this is true; the converse, however, is not true in this simplicity. One could, for instance, use an error-correcting block code for the transmission of the cryptogram. For the adversary, the encoded cryptogram is the real cryptogram, that is, as far as the mathematical model is concerned, the cryptogram contains redundancy and is non-random. In general, a cryptogram may contain two kinds of information for the adversary: *Useless information,* that has nothing to do whith the original message – the information coming from the error-correcting code; *useful infor-*

mation giving clues about the message. For the cryptanalyst – and for secrecy theory – these may be difficult to distinguish.

It is our hope that this paper will initiate a re-examination of the discussion about a general theory of secrecy systems, incorporating not only considerations from probability theory and information theory, but also looking at issues for which the theories of computational complexity and program-size complexity may provide an appropriate setting. We have developed a small general formal framework, in which aspects of secrecy can be expressed uniformly, thus making it easier to relate various approaches to each other. In the spirit of Shannon's foundational work, we believe that some such general formal framework – whether this or another better one – is required to make *proofs* about secrecy achieved by information transmission systems possible.

References

1. F. L. Bauer: *Kryptologie, Methoden und Maximen.* Springer-Verlag, Berlin, 1994.
2. B. Beckett: *Introduction to Cryptology.* Blackwell Scientific Publications, Oxford, 1988.
3. H. Beker, F. Piper: *Cipher Systems The Protection of Communications.* Northwood Publications, London, 1982.
4. T. A. Berson: Long key variants of des. In D. Chaum, R. L. Rivest, A. T. Sherman (editors): *Advances in Cryptology – Proceedings of CRYPTO '82.* 311–313, New York, 1983. Plenum Press.
5. T. Beth, P. Heß, K. Wirl: *Kryptographie.* Teubner, Stuttgart, 1983.
6. G. R. Blakley, I. Borosh: Rivest-shamir-adleman public key cryptosystems do not always conceal messages. *Comp. & Maths. with Appls.* **5** (1979), 169–178.
7. M. Blum: A machine-independent theory of the complexity of recursive functions. *J. Assoc. Comput. Mach.* **14** (1967), 322–336.
8. A. Bosselaers, B. Preneel (editors): *Integrity Primitives for Secure Information Systems. Final Report of RACE Integrity Primitives Evaluation RIPE-RACE 1040.* Springer-Verlag, Berlin, 1995.
9. G. Brassard: A note on the complexity of cryptography. *IEEE Trans. Inform. Theory* **IT-25** (1979), 232–233.
10. C. Calude: *Theories of Computational Complexities.* North-Holland, Amsterdam, 1988.
11. C. Calude: *Information and Randomness – An Algorithmic Perspective.* Springer-Verlag, Berlin, 1994.
12. C. Calude: What is a random string? *J. UCS* **1** (1995), 48–66.
13. C. Calude, H. Jürgensen: Randomness-preserving transformations. Manuscript, 32 pp., 1995.
14. J. M. Carroll, M. Kantor: Evaluating cryptographic strategies. In W. Caelli (editor): *Computer Security in the Age of Information.* 119–134. Elsevier Science Publishers B.V.(North-Holland), 1988.

15. G. J. Chaitin: *Information, Randomness and Incompleteness. Papers on Algorithmic Information Theory.* World Scientific, Singapore, second ed., 1987, 1990.
16. G. J. Chaitin: On the length of programs for computing finite binary sequences: Statistical considerations. *J. Assoc. Comput. Mach.* **16** (1969), 145–159. Reprinted in [15], 239–255.
17. D. W. Davies: How to use the des safely. In J. B. Grimson, H.-J. Kugler (editors): *Computer Security: The Practical Issues in a Troubled World – Proceedings of the Third IFIP International Conference on Computer Security.* 371–378, Amsterdam, 1985. North-Holland.
18. D. E. Denning: *Cryptography and Data Security.* Addison-Wesley Publishing Company, Reading, MA, 1982.
19. E. Fischer: A theoretical measure of cryptographic performance. *Cryptologia* **5**(1) (1981), 59–62.
20. C. C. Foster: *Cryptanalysis for Microcomputers.* Hayden Book Company, Inc., Rochelle Park, NJ, 1982.
21. L. C. Guillou, M. Davio, J.-J. Quisquater: Public-key techniques: Randomness and redundancy. *Cryptologia* **13**(2) (1989), 167–189.
22. P. R. Halmos: *Measure Theory.* Springer-Verlag, Berlin, 1974.
23. M. E. Hellman: An extension of the Shannon theory approach to cryptography. *IEEE Trans. Inform. Theory* **IT-23** (1977), 289–294.
24. B. S. K. Jr., R. L. Rivest, A. T. Sherman: Is des a pure cipher? (results of more cycling experiments on des) (preliminary abstract). In G. Goos, J. Hartmanis (editors): *Advances in Cryptology – Proceedings of CRYPTO '85.* 212–222, Berlin, 1986. Springer-Verlag.
25. H. Jürgensen: Language redundancy and the unicity point. *Cryptologia* **7** (1983), 37–48.
26. H. Jürgensen, S. Konstantinidis: Codes. In G. Rozenberg, A. Salomaa (editors): *Handbook of Formal Language Theory.* Springer-Verlag, Berlin, to appear.
27. H. Jürgensen, M. Kunze: A complexity-theoretic approach to cryptography. Manuscript, 43 pp.
28. H. Jürgensen, D. Matthews: Some results on the information theoretic analysis of cryptosystems. In D. Chaum (editor): *Advances in Cryptology, Proceedings of CRYPTO 83, Santa Barbara, 1983.* 303–356, New York, 1984. Plenum Press.
29. D. Kahn: *The Codebreakers.* Macmillan Publishing Co., New York, 1967.
30. L. R. Knudsen: New potentially 'weak' keys for des and loki (extended abstract). In A. D. Santis (editor): *Advances in Cryptology – Proceedings of EUROCRYPT '94.* 419–424, Berlin, 1995. Springer-Verlag.
31. A. N. Kolmogorov: Three approaches for defining the concept of 'information quantity'. *Problemy Peredachi Informatsii* **1** (1965), 3–11, in Russian.
32. J. C. Lagarias: Pseudorandom number generatos in cryptography and number theory. In C. Pomerance (editor): *Proceedings of Symposia in Applied Mathematics Cryptology and Computational Number Theory*, 42. 115–143,

Providence, Rhode Island, 1990. American Mathematical Society.

33. M. Li, P. Vitányi: *An Introduction to Kolmogorov Complexity and Its Applications*. Springer-Verlag, Berlin, 1993.
34. R. Lidl, H. Niederreiter: *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, 1986.
35. J. L. Massey: An introduction to contemporary cryptology. *Proceedings of the IEEE* **76**(5) (1988), 533–549.
36. L. Robbins. Ph. D. thesis, in preparation.
37. B. Schneier: *Applied Cryptography Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, New York, 1994.
38. C. E. Shannon: Communication theory of secrecy systems. *Bell System Tech. J.* **28** (1949), 656–715.
39. D. R. Stinson: *Cryptography Theory and Practice*. CRC Press, Boca Raton, 1995.
40. G. S. Vernam: Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. American IEE* **XLV** (1926), 109–115.
41. K. Weihrauch: *Computability. EATCS Monographs on Theoretical Computer Science* **9**. Springer-Verlag, Berlin, 1987.