Cryptographic Security of Individual Instances

Luís Antunes* Sophie Laplante+ Alexandre Pinto* Liliana Salvador*
* DCC-FC & LIACC
University of Porto, Portugal
+ Univ Paris-Sud; LRI, France *

May 7, 2007

Abstract

There are two principal notions of security for cryptographic systems. For a few systems, they can be proven to have perfect secrecy against an opponent with unlimited computational power, in terms of information theory. However, the security of most systems, including public key cryptosystems, is based on complexity theoretic assumptions. In both cases there is an implicit notion of average-case analysis. In the case of conditional security, the underlying assumption is usually average-case, not worst case hardness. And for unconditional security, entropy itself is an average case notion of encoding length.

Kolmogorov complexity (the size of the smallest program that generates a string) is a rigorous measure of the amount of information, or randomness, in an individual string $x$. By considering the time-bounded Kolmogorov complexity (program limited to run in time $t(|x|)$) we can take into account the computational difficulty of extracting information. We present a new notion of security based on Kolmogorov complexity. The first goal is to provide a formal definition of what it means for an individual instance to be secure. The second goal is to bridge the gap between information theoretic security, and computational security, by using time-bounded Kolmogorov complexity.

In this paper, we lay the groundwork of the study of cryptosystems from the point of view of security of individual instances by considering three types of information-theoretically secure cryptosystems: cipher systems (such as the one-time pad), threshold secret sharing, and authentication schemes.

Keywords: Perfect secrecy, Kolmogorov complexity.

1 Introduction

Classical information theory originated in Shannon’s 1948 paper “A mathematical theory of communication” [Sh49], where the author defined the notion of entropy and showed that it corresponds to the amount of information associated with any given statistical event. Another notion of information was proposed in the 60’s, independently by Solomonoff, Kolmogorov and Chaitin [Sol64, Kol65, Cha66]. This quantity is now known as Kolmogorov complexity and is defined as the length of the shortest program that can produce a given string. Unlike entropy, this quantity depends exclusively on the string, and not on the probability with which it is sampled from some given distribution. As such, Kolmogorov complexity measures the intrinsic information in a given string.

*Partially supported by KCrypt (POSC/ELIA/60819/2004), the grant SFRH/BD/13124/2003 from FCT and funds granted to LIACC through the Programa de Financiamento Plurianual, FCT and Programa POSI, as well as ANR Blanc AlgoQP.
Traditionally, information theory has been used in the analysis of unconditionally secure cryptographic systems. However, because of the inherent statistical nature of information theory, two distributions may have nil information about each other and yet particular instances of the plaintext and ciphertext have large mutual information in the individual sense. Even though such cases are probabilistically rare, and don’t influence the information theoretic security, they still correspond to situations we’d rather avoid in practice.

In this paper, we give a notion of individual security, using Kolmogorov complexity to formalize what is meant by an ad hoc attack on an individual instance.

We believe this is a more realistic model of attack, since in practice, an attacker may not necessarily attempt to break all instances of a cryptosystem, but is likely to be willing to invest a lot of resources in breaking a single instance.

We then analyse some cryptographic protocols, in order to determine which are the truly secure instances of the cryptosystem. We consider three basic types of information theoretically secure cryptographic systems: cipher systems, threshold secret sharing schemes, and authentication schemes.

Our first goal is to provide a finer grained notion of security than the traditional information theoretic security. For each of the settings that we consider, we first give a Kolmogorov complexity based definition of security of an individual instance. Then we prove that security in this sense implies security in the traditional sense, by showing that if sufficiently many instances of a system are individually secure, then the system is also information theoretically secure. This implication is not perfect in the case of cypher systems and secret sharing, because we cannot avoid the existence of instances with very significative mutual information of the ciphertext about the plaintext (and equivalent notions for the secret sharing system). Finally, we identify the high-security instances of specific systems, using again properties derived from Kolmogorov complexity.

Our second goal in this work is to bridge the gap between information theoretic security, which does not take into account the resources necessary to extract information, and computational security. This paper takes a first step towards using tools from time-bounded Kolmogorov complexity to analyse cryptographic systems.

By providing a computable (though admittedly not efficient) method to establish the level of security of a particular instance of the system, we can guarantee that an instance of a cryptosystem is secure against a time-bounded adversary. We give such results for the one-time pad as well as for authentication schemes.

2 Preliminaries

2.1 Entropy

Information theory quantifies the a priori uncertainty about the results of an experiment. It is based on Shannon’s entropy and corresponds to the number of bits necessary on average to describe an outcome from an ensemble.

Let \( X, Y \) be random variables. The probability that \( X \) takes on the value \( x \) from a finite or countably infinite set \( \mathcal{X} \) is denoted by \( p_X(x) \); the mutual probability, the probability that both \( x \) and \( y \) occur, by \( p_{XY}(x, y) \) and the conditional probability, the probability that \( x \) occurs knowing that \( y \) has occurred by \( p_{XY}(x|y) \). Two random variables \( X \) and \( Y \) are independent if and only if for all \( x \in X \) and \( y \in Y \) \( p_{XY}(x, y) = p_X(x) \times p_Y(y) \). For convenience, \( p_{XY}(x, y), p_{XY}(x|y) \) and \( p_X(x) \) are denoted, respectively by \( p(x, y), p(x|y) \) and \( p(x) \).

**Definition 1** Let \( X \) and \( Y \) be random variables.

- **Entropy:** \( H(X) = - \sum_{x \in \mathcal{X}} p(x) \log p(x) \), and \( H(X|Y) = \sum_{y \in \mathcal{Y}} p(y) H(X|Y = y) \).
• **Mutual information**: \( I(X; Y) = H(X) - H(X|Y) \).

We recall a few properties of entropy.

**Theorem 2** Let \( X \) and \( Y \) be random variables.

1. **Conditional entropy**: \( H(Y|X) \leq H(Y) \) and \( X \) and \( Y \) are independent if and only if equality holds.
2. **Additivity**: \( H(X, Y) = H(Y) + H(X|Y) \).
3. **Symmetry of information**: \( I(X; Y) = I(Y; X) \).

### 2.2 Kolmogorov complexity

We briefly introduce Kolmogorov complexity only at the level of generality needed. For more details, the textbook by Li and Vitányi [LV97] and Peter Gács’ lecture notes [G88] are good references.

We consider only the binary alphabet \( \Sigma = \{0, 1\} \). Our computation model will be *prefix free* Turing machines: Turing machines with a one-way input tape (the input head can only read from left to right), a one-way output tape and a two-way work tape. A set of strings \( A \) is prefix-free if there are no strings \( x \) and \( y \) in \( A \) where \( x \) is a proper prefix of \( y \). The function \( \log \) denotes \( \log_2 \), \( |.| \) denotes the length of a string and \( \# \) the cardinality of a set. A Turing Machine is prefix-free if its domain (set of inputs on which it halts) is prefix-free.

We present next the necessary definitions:

**Definition 3 (Kolmogorov complexity)** Let \( U \) be a fixed universal prefix-free Turing machine.

- **Conditional Kolmogorov complexity**: \( K(x|y) = \min_p \{|p| : U(p, y) = x\} \).
- **Mutual information**: \( I_K(x : y) = K(x) + K(y) - K(x, y) \).

The default value for \( y \) is the empty string \( \epsilon \). A different universal machine \( U \) may affect the program size \( |p| \) by at most a constant additive factor.

We list the properties of Kolmogorov complexity that we need.

**Theorem 4**

1. **Upper bound**: For each \( n \), \( \max\{K(x) : |x| = n\} = n + K(n) + O(1) \).
2. **Incompressibility**: For any string \( y \), for each fixed constant \( r \), the number of \( x \) of length \( n \) with \( K(x|y) \leq n - r \) does not exceed \( 2^{n-r} \).
3. **Additivity**: Up to an additive constant, \( K(x, y) = K(x) + K(y|x^*) = K(y) + K(x|y^*) \), where \( x^* \) is the first shortest program that produces \( x \).
4. **Conditional additivity**: Up to an additive constant, \( K(x, y|z) = K(x|z) + K(y|x, K(x|z), z) = K(y|z) + K(x|y, K(y|z), z) \).
2.3 Resource-bounded Kolmogorov complexity

The main disadvantage of using Kolmogorov complexity in many settings (including the one addressed in this paper) is that determining the Kolmogorov complexity of a given string is not a computable task. However, resource-bounded Kolmogorov complexity [Har83], where the programs considered always halt before expending their allocated resource bound, does not suffer from this drawback. More importantly, it gives a notion of information theory that takes complexity limitations into account, bridging the gap between complexity and information theory.

**Definition 5 (Time-bounded Kolmogorov complexity)** Let $U$ be a fixed universal Turing machine, and $t$ be a fully-constructible time bound. Then for any string $x, y \in \Sigma^*$, the $t$ time-bounded complexity is $K^t(x|y) = \min_p \{|p| : U(p, y) = x \text{ and } U(p, y) \text{ runs in at most } t(|x| + |y|) \text{ steps}\}$.

This definition corresponds to time-bounded computation, but one may also define other measures, for instance for space bounded computation, and so on. For this paper we require a variant where the program has the same computing ability as the class $AM$, where the computation is done in probabilistic polynomial time with bounded error (Arthur), with the help of nondeterminism (Merlin).

**Definition 6 (CAM complexity)** Let $U$ be a fixed universal nondeterministic Turing machine. Then for any string $x, y \in \Sigma^*$, for a polynomial $t$, the $t$-time-bounded AM decision complexity $CAM^t(x|y)$ is the length of the smallest program $p$ such that

1. $\forall r, U(p, y, r)$ runs in at most $t(|x| + |y|)$ steps,
2. with probability at least $2/3$ over the choice of $r$, $U(p, y, r)$ has at least one accepting path, and
   $U(p, y, r) = x$ on all of the accepting paths.

We give a bound to the time that it takes to compute $K^t(x)$:

**Theorem 7** For $t$ a fully-constructible time bound, $K^t(x)$ can be computed in time $O(t(|x| \cdot 2^{|x|})$.

Many facts about Kolmogorov complexity, such as existence and number of incompressible strings, are also true for resource bounded Kolmogorov complexity. However, one important property of Kolmogorov complexity that is believed to fail to hold in resource bounded models is symmetry of information. Symmetry of information states that information in $x$ about $y$ is the same as information in $y$ about $x$. Note that this naturally comes into play in a cryptographic setting: consider the case where $y$ is the result of applying a one-way permutation to $x$. Without any time bounds, the permutation can be inverted. However, this no longer works for time-bounded computation. Intuitively, for the same reason that one-way functions are believed to exist, it is believed that symmetry of information fails to hold for polynomial-time bounded computation.

However, weaker versions of symmetry of information are known to hold for resource bounded Kolmogorov complexity.

**Theorem 8 (Time-bounded symmetry of information, [LR05])** For any polynomial time bound $t$, there exists a polynomial time bound $t'$ such that

$$K^t(y) + K^t(x|y) \geq CAM^{t'}(x) + CAM^{t'}(y|x) - O(\log^3(|x| + |y|)).$$
2.4 Entropy vs Kolmogorov complexity

There is a very close relation between these two measures: Shannon’s entropy is the expected value of
Kolmogorov complexity for computable distributions. In this sense, Kolmogorov complexity is a sharper
notion than entropy. The following theorem follows from Corollary 4.3.2 and Theorem 8.1.1 in [LV97].

**Theorem 9** Let $X,Y$ be random variables over $\mathcal{X}, \mathcal{Y}$. For any computable probability distribution $\mu(x,y)$
over $\mathcal{X} \times \mathcal{Y}$, $0 \leq \left( \sum_{x,y} \mu(x,y)K(x|y) - H(X|Y) \right) \leq K(\mu) + O(1)$.

**Proof:** Let $\mu_Y$ and $\mu_X$ be the marginal probability distributions over $\mathcal{Y}$ and $\mathcal{X}$ respectively. Similarly,
denote by $\mu_{X|Y}$ and $\mu_{Y|X}$ the conditional probability distributions. For the first inequality, $H(X|Y) = \sum_y \mu_Y(y) \sum_x \mu_{X|Y}(x)K(x|y) = \sum_x \mu_X(x)K(x|y)$ where the last inequality follows from the Noiseless Coding Theorem (see [LV97]) since $y$ is a fixed string.

For the second direction, Corollary 4.3.2 in [LV97] states that $K(x|y) \leq \log 1/\mu_{X|Y}(x|y) + K(\mu) + O(1)$. Therefore,

$$\sum_y \mu_Y(y) \sum_x \mu_{X|Y}(x|y)K(x|y) \leq \sum_y \mu_Y(y) \sum_x \mu_{X|Y}(x|y) \log 1/\mu_{X|Y}(x|y) + K(\mu) + O(1)$$

$$= \sum_{x,y} \mu(x,y) \log 1/\mu_{X|Y}(x|y) + K(\mu) + O(1)$$

$$= H(X|Y) + K(\mu) + O(1)$$

By $K(\mu)$, we mean the length of the smallest probabilistic algorithm $A$ that outputs $x$ with probability $\mu(x)$. Note that $K(\mu)$ is a constant $c_{\mu}$ depending only on the (computable) conditional probability of $X$ and $Y$, but not on the particular value of $x$ [Cha75]. The $O(1)$ term depends only on the reference universal prefix machine.

An analogous result for mutual information holds.

**Theorem 10 ([GV04])** Let $X,Y$ be random variables over $\mathcal{X}, \mathcal{Y}$. For any computable probability distribution $\mu(x,y)$ over $\mathcal{X} \times \mathcal{Y}$, $I(X;Y) = K(\mu) \leq \sum_{x,y} \mu(x,y) I_K(x : y) \leq I(X;Y) + 2K(\mu)$. When $\mu$ is given, then $I(X;Y) = \sum_{x,y} \mu(x,y) I_K(x : y|\mu) + O(1)$.

3 Cipher Systems

We begin this study by examining the simplest cryptographic systems: cipher systems. In this section,
we show what makes a cipher system secure both with entropy and Kolmogorov complexity and give an
example system that is secure under both definitions: the one-time pad.

3.1 Information theoretic security of cipher systems

A private key cipher system is a five tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, e, d)$, where $\mathcal{M}$ is the plaintext space, $\mathcal{C}$ is the ciphertext space, $e : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$ is the encryption algorithm, $d : \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M}$ is the decryption algorithm and $d(k, e(k, m)) = m$. We use uppercase $M, C, K$ to denote random variables over the message, ciphertext, and key spaces, and lower case $m, c, k$ for individual instances of the cipher system.

A system is called *computationally secure* if it is secure against an adversary with bounded resources and it is called *information-theoretically (or unconditionally) secure* if the ciphertext provides no information about the plaintext, regardless of the adversary’s computational power.
Definition 11 A private key cipher system has $\delta$ security if $I(M; C) \leq \delta$.

When $\delta = 0$, the classical notion of perfect security states that the \textit{a posteriori} probability that a message $m$ was sent, given that we observe ciphertext $c$, is equal to the \textit{a priori} probability that message $m$ is sent.

3.2 Instance security for cipher systems

We use Kolmogorov complexity to define what it means for an individual instance of a cryptographic system to be secure. Intuitively, an instance $m, k$ is secure if there is no \textit{ad hoc} attack that can find the plaintext, even when given this particular ciphertext and full information about the distribution of the messages. Of course, we cannot rule out the \textit{ad hoc} attack where the attacker already knows the message and prints it out. But we define security in such a way that the length of the \textit{ad hoc} program that computes the plaintext, given the ciphertext, must be at least as long as any shortest program that prints the plaintext – so any \textit{ad hoc} attack may as well have a description of the plaintext hard-coded into its program.

Definition 12 Let $(\mathcal{M}, \mathcal{C}, \mathcal{K}, e, d)$ be a cipher system, and $\mu$ be a distribution over $\mathcal{M} \times \mathcal{K}$. An instance $m, k \in \Sigma^n$ of the cipher system is $\gamma$-secure if $I_K(m : e(k, m) | \mu) \leq \gamma$.

We say that a $\gamma$-secure instance has $\gamma$ secrecy. We now prove that if enough instances of a cipher system are secure, then the system is information theoretically secure. This result establishes that instance security is a sharper notion than information theoretic security.

Theorem 13 For any private key cipher system $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$, for any independent $M, K$ over $\mathcal{M}, \mathcal{K}$ with distribution $\mu$, if the probability that an instance is $\gamma$ secure is at least $(1-\epsilon)$, then the system has $\gamma + \epsilon \log(\# \mathcal{M})$ secrecy, in the information theoretic sense. Furthermore, if for any $t, \gamma < t \leq n, \mu\{|m, k : I_K(m : e(k, m) | \mu) = t\} = O(f(t))$, then the system has $\gamma + \sqrt{\epsilon \sum_{\gamma < t \leq n} t^2 O(f(t))}$ security.

Proof: Let $M, K$ be independent random variables with computable distribution $\mu$. By Theorem 10 we have that up to an additive constant, $I(M; C) \leq \sum_{m,k} \mu(k, m) I_K(m : e(m, k) | \mu)$. We separate the sum into two parts, the secure instances and the others. Let $G$ be the set of $\gamma$-secure instances.

$$I(M; C) \leq \sum_{m,k \in G} \mu(k, m) I_K(m : e(m, k) | \mu) + \sum_{m,k \notin G} \mu(k, m) I_K(m : e(m, k) | \mu)$$

$$\leq \gamma \sum_{m,k \in G} \mu(k, m) + \sum_{m,k \notin G} \mu(k, m) [K(m | \mu) - K(m | e(m, k), \mu)]$$

$$\leq \gamma + \sum_{m,k \notin G} \mu(k, m) K(m | \mu)$$

$$\leq \gamma + \epsilon \log(\# \mathcal{M}).$$

If in addition we have $\mu\{|m, k : I_K(m : e(k, m) | \mu) = t\} = O(f(t))$, then as before,

$$I(M; C) \leq \gamma + \sum_{m,k \in G} \mu(k, m) I_K(m : e(m, k) | \mu)$$

$$= \gamma + \sum_{\gamma < t \leq n} t \cdot \mu\{|m, k : I_K(m : e(k, m) | \mu) = t\}$$

$$\leq \gamma + \sum_{\gamma < t \leq n} t \sqrt{f(t)} \cdot \sqrt{\mu\{|m, k : I_K(m : e(k, m) | \mu) = t\}}$$
Recall that the Cauchy-Schwarz inequality states that $\sum_i a_i b_i \leq \sqrt{\left(\sum_i a_i^2\right) \left(\sum_i b_i^2\right)}$.

$$I(M; C) \leq \gamma + \sum_{\gamma < t \leq n} t^2 f(t) \sum_{\gamma < t \leq n} \mu(\{m, k : I_K(m : e(k, m)|\mu) = t\})$$

$$\leq \gamma + \sum_{\gamma < t \leq n} t^2 f(t) \sqrt{\epsilon},$$

since $\sum_{\gamma < t \leq n} \mu(\{m, k : I_K(m : e(k, m)|\mu) = t\}) = \sum_{m, k \in G} \mu(m, k) \leq \epsilon$.

### 3.3 Instance security of one-time pad

In the previous section, we have given a definition of security of individual instances of cipher systems, and shown that if sufficiently many instances are secure, then the system is secure in the traditional sense, thereby establishing that our definition is a refinement of the standard notion of security.

In this section, we illustrate this with a specific cipher system: the one-time pad. First (Theorem 14), we identify a set of secure instances according to our definition. These are the keys with maximum Kolmogorov complexity, together with messages that have no common information with the key. Then (Corollary 15), we show that this set is indeed large enough to imply security in the information theoretic sense.

**Theorem 14** Let $\mu$ be a distribution over $\Sigma^n \times \Sigma^n$. Let $m, k \in \Sigma^n$ and consider $e(k, m) = m \oplus k$, an instance of the one-time pad, with $K(k|\mu) \geq n - \alpha$, and $K(m, k|\mu) \geq K(m|\mu) + K(k|\mu) - \beta$. Then the instance has $\alpha + \beta$ secrecy.

**Proof:** By Theorem 4 (item 4), up to an additive constant,

$$K(m|m \oplus k, \mu) \geq K(m|m \oplus k, K(m \oplus k|\mu), \mu) = K(m|\mu) - K(m \oplus k|\mu) + K(m \oplus k|m, K(m|\mu), \mu) = K(m|\mu) - K(m \oplus k|\mu) + K(k|m, K(m|\mu), \mu) \geq K(m|\mu) - n + K(k|m, K(m|\mu), \mu) \text{ (using } |m \oplus k| = n) \geq K(m|\mu) - n + K(m|\mu) - K(m|\mu) \text{ (by Theorem 4 (item 4))} \geq K(m|\mu) - n + n - \alpha - \beta \text{ (by hypothesis)} = K(m|\mu) - \alpha - \beta$$

Combining this with Theorem 13, we have the following corollary.

**Corollary 15** Let $\mu_M$ be a computable distribution over $\mathcal{M}$, and $\mu_K$ be the uniform distribution. Then one-time pad is $O(1)$-secure in the information theoretic sense.

**Proof:** Let $\mu(m, k) = \mu_M(m) \cdot \mu_K(k)$. Let $G_{\alpha, \beta} = \{(m, k) : K(k|\mu) \geq n - \alpha \text{ and } K(m, k|\mu) \geq K(m|\mu) + K(k|\mu) - \beta\}$. By Theorem 14, we know that all instances in $G_{\alpha, \beta}$ have $\alpha + \beta$ secrecy. We show that $\mu((\mathcal{M} \times \mathcal{K}) \setminus G) \leq (2^{-\alpha} + 2^{-\beta})$. 


Observe that $\mathcal{M} \times \mathcal{K} \setminus G \subseteq B_\alpha \cup B_\beta$, where
\[
B_\alpha = \{ (m, k) : K(k|\mu) < n - \alpha \}, \\
B_\beta = \{ (m, k) : K(m, k|\mu) < K(m|\mu) + K(k|\mu) - \beta \}.
\]
By Theorem 4 (item 2), $\mu(B_\alpha) \leq 2^{-\alpha}$.

**Claim 1** $\mu(B_\beta) \leq 2^{-\beta}$

By definition, $\mu(B_\beta) = \sum_{m, k \in B_\beta} \mu(m, k) = \sum_{m} \mu_M(m) \sum_{k, m, k \in B_\beta} \mu_K(k)$. By Theorem 4 (item 4), $K(m, k|\mu) = K(m|\mu) + K(k|m, K(m|\mu), \mu)$, so when $m$ is fixed, the second summation runs over $k$ with $K(k|m, K(m|\mu), \mu) < K(k|\mu) - \beta$. By Theorem 4 (item 2), there are at most $2^{K(k|\mu) - \beta}$ terms in the inner summation. Therefore, using $\mu_K(k) = 2^{-n}$ and $K(k|\mu) \leq n$, $\mu(B_\beta) \leq \sum_m \mu_M(m)2^{K(k|\mu) - \beta} \mu_K(k) \leq 2^{-\beta}$, which concludes the proof of the claim.

**Claim 2** For any $t, \gamma < t \leq n$, $\mu(\{m, k : I_K(m : e(k, m)|\mu) = t\}) \leq 2^{-t}$.

The claim follows from the fact that
\[
I_K(m : e(k, m)|\mu) = K(e(k, m)|\mu) - K(e(k, m)|m, K(m|\mu), \mu) \\
\leq n - K(e(k, m)|m, K(m|\mu), \mu) \\
= n - K(k|m, K(m|\mu), \mu)
\]
where the final equality holds in the case of the one-time pad. Therefore $\mu(\{m, k : I_K(m : e(k, m)|\mu) = t\}) \leq \mu(\{m, k : K(k|m, K(m|\mu), \mu) \leq n - t\}) \leq 2^{n-t} \cdot 2^{-n} = 2^{-t}$.

We can apply Theorem 13 with $\gamma = \alpha + \beta$ and $\epsilon = 2^{-\alpha} + 2^{-\beta}$. Therefore, the system has $\gamma + \sqrt{\epsilon \sum_{\gamma \leq t} t^2 2^{-t}} = \alpha + \beta + O(1)$ security since the series converges. If $\alpha = \beta = O(1)$, then we can conclude that the one-time pad is $O(1)$-secure.

### 3.4 Resource-bounded instance security of one-time pad

Of more practical importance, we prove that if one is willing to expend the time necessary to produce a secure instance, then it is guaranteed to be secure against an adversary that is limited in the amount of time at its disposal to decrypt the instance.

**Definition 16** Let $(\mathcal{M}, \mathcal{C}, \mathcal{K}, e, d)$ be a cipher system. An instance $m, k$ of the cipher system is $\gamma$-secure against a $t$-time-bounded adversary if $K^t(m|e(k, m)) \geq K^t(m) - \gamma$.

**Theorem 17** For any polynomial time bound $t$, there is a time bound $t'$ polynomial in $t$ such that the following holds: if $m, k \in \Sigma^a$ and $e(k, m) = m \oplus k$ be an instance of a one time pad scheme, such that $CAM^{t'}(k, m) \geq n + K^t(m) - \alpha$, then the instance has $\log O(1) n + \alpha$ secrecy against a $t$-time-bounded adversary.
Proof: The proof is similar to Theorem 14, except for the application of time bounded symmetry of information, Theorem 8.

\[ K^t(m|m \oplus k, \mu) \geq K^t(m) \]  
\[ = CAM^t(m) + CAM^t(m \oplus k, \mu^*) \]  
\[ \geq CAM^t(m) - K^t(m \oplus k, \mu) - O(\log^3(\|x\| + \|y\|)) \]  
\[ \geq CAM^t(m, k) - n - O(\log^3(\|x\| + \|y\|)) \]  
\[ \geq K^t(m) - \alpha - O(\log^3(\|x\| + \|y\|)) \]

To compute the CAM complexity of a key and message pair, one could simulate all CAM programs up to length 2n (an exponential number) to rule out the existence of a short program. This is by no means efficient; however, it is computable.

4 Threshold Secret Sharing Schemes

In this section, we revisit threshold secret sharing schemes, invented independently in 1979 by Shamir ([Sha79]) and Blakley ([Bla79]), and analyse the security of individual instances.

4.1 Information theoretic secrecy of secret sharing schemes

Let \( q, w \) be positive integers, \( q \leq w \). \((K, S, d, r)\) is a \((q, w)\) threshold scheme if \( d : K \rightarrow S^w \) produces \( w \) shares of a key \( K \in K \) in such a way that any \( q \) participants can compute the value of \( K \) by using the reconstruction function \( r \), but no group of at most \( q - 1 \) participants can do so.

Let \( \mathcal{P} = \{P_i, 1 \leq i \leq w\} \) denote the set of participants, and let \( D \notin \mathcal{P} \) be the dealer, that is a special participant who chooses the value of the key \( K \). Let \( \mathcal{B} = (i_1, \ldots, i_j) \) be any set of participants that want to reconstruct the key, where \( j \leq w \). Let \( d(K) = \{(x_i, y_i) : 1 \leq i \leq w\} \) be the set of all shares distributed by the dealer, where the values \( x_i \) are public and each \( y_i \) is known only by its holder. The values \( y_i \) are determined from the secret information held by \( D \), which includes at least the secret \( K \). Let \( X \) be a random variable over the possible values for \( x_i \), and \( Y \) be analogous for \( y_i \). Then, \( Y \) is totally dependent of \( X \), that is, \( H(X, Y) = H(X) \).

Definition 18 A \((q, w)\) threshold scheme \((K, S, d, r)\) has \( \delta \) security if:
- If \(|\mathcal{B}| \geq q \) then \( H(K|x_{i_1}, \ldots, x_{i_{|\mathcal{B}|}}, y_{i_1}, \ldots, y_{i_{|\mathcal{B}|}}) = 0 \)
- If \(|\mathcal{B}| < q \) then \( H(K|x_{i_1}, \ldots, x_{i_{|\mathcal{B}|}}, y_{i_1}, \ldots, y_{i_{|\mathcal{B}|}}) \geq H(K) - \delta \)

4.2 Individual secrecy of secret sharing schemes

We now give an individual analysis of perfect security based on Kolmogorov complexity.

To simplify reading, we use the following notation

Definition 19 Let \([w] = 1, 2, \ldots, w\) represent the set of all participants. Let \( x y_w = (x_1, y_1, \ldots, x_w, y_w) \) represent the concatenation of all shares in the same ordering as used for the participants. For any \( \mathcal{B} \subseteq [w] \), let \( x y_{\mathcal{B}} = x y_w | \mathcal{B} \) be the projection of \( x y_w \) onto the participants selected by \( \mathcal{B} \), that is, \( x y_{\mathcal{B}} = (x_{i_1}, y_{i_1}, \ldots, x_{i_j}, y_{i_j}) \) where \( \mathcal{B} = \{i_1, i_2, \ldots, i_j\} \) for some \( j \leq w \). For any instance \((k, x y_w)\)
and \( B \subseteq [n] \), \((k, xy_B^{q-1})\) is a \(|B|\)-arrangement of the instance \((k, xy_w)\). We also write \( xy_{q-1} \) to represent any concatenation of some \( q - 1 \) distinct pairs of \( xy_w \), without considering which subset of \([w]\) originated it.

We need a shorthand definition for the remainder of this section.

**Definition 20** Fix an integer \( w \) and another integer \( q \leq w \). Then, the notation \( \binom{[w]}{q-1} \) represents the set of subsets of \([w]\) that have \( q - 1 \) elements. Formally, \( \binom{[w]}{q-1} = \{ B : B \subseteq [w], \#B = q - 1 \} \).

**Definition 21** Let \((K, S, d, r)\) be a \((q, w)\) threshold scheme and \( \mu \) a distribution over \( K \times S^w \), and \((k, xy_w)\) an instance of this scheme.

1. \((k, xy_B^{q-1})\) is \( \gamma \)-secure against an attack from \( B \) if \( I_K(k:xy_B^{q-1}|\mu) \leq \gamma \).
2. \((k, xy_w)\) is \((\gamma, \phi)\)-secure if \( \Pr_{B \in \binom{[w]}{q-1}}[I_K(k:xy_B^{q-1}|\mu) \leq \gamma] \geq 1 - \phi \) under the uniform distribution over \( q - 1 \) arrangements.

**Theorem 22** For any \((q, w)\)-threshold scheme where \( K \) is the set of keys and \( S = \{(x_i, y_i) : 1 \leq i \leq w\} \) the set of all shares, for any independent variables \( K, X^w = X \times \cdots \times X \) over \( K, S^w \) with distribution \( \mu(k, xy_w) = \mu_k(k) \cdot \mu_w(xy_w) \). If the probability that any given instance is \((\gamma, \phi)\)-secure is at least \((1 - \epsilon)\), then the system has \((\gamma + (\epsilon + \phi) \log \#K)\) secrecy, in the information theoretic sense.

**Proof:**

1. By definition of \((q, w)\)-threshold secret sharing scheme, if \(|B| \geq q\) the attackers can effectively compute the secret key merely by pooling their private and public shares. This means there is a function that computes \( K \) from any set of \( q \) distinct points \((x_i, y_i)\), and therefore \( H(K|xy_w|B) = 0 \).

2. Let \( xy_w = \langle (x_1, y_1), \ldots, (x_w, y_w) \rangle \) and let \((k, xy_w)\) represent a particular instance of the system.

We show that \( I(K; X^wY^w) \) is bounded above by \( \gamma + (\epsilon + \phi) \log \#K \), using the upper bound given by Theorem 10, as the average of Kolmogorov mutual information. We first consider fixed instances of the scheme, then take the average over all instances.

For any instance \((k, xy_w)\), let

\[
\tilde{I}(k : xy_w | \mu) = \sum_{B \in \binom{[w]}{q-1}} \mu'(xy_w | B | xy_w) I_K(k : xy_w | B | \mu),
\]

where \( \mu' \) is derived from \( \mu \) in the natural way, as the conditional marginal distribution of \( \mu \).

Let \( G \) be the set of instances that are \((\gamma, \phi)\)-secure. Then, for all \((k, xy_w) \in G\),

\[
\tilde{I}(k : xy_w | \mu) = \sum_{B : I_K(k : xy_w | B) \leq \gamma} \mu'(xy_w | B | xy_w) I(k : xy_w | B | \mu)
+ \sum_{B : I_K(k : xy_w | B) > \gamma} \mu'(xy_w | B | xy_w) I(k : xy_w | B | \mu)
\leq \gamma + \phi \cdot \log \#K
\]
We apply Theorem 10 using the distribution $\nu(k, x y) = \mu_K(k) \mu_w(x y) \mu'(x y_{q-1} | x y_w)$, so
\[
\sum_{k, x y_w} \mu(k, x y_w) \tilde{I}(k : x y_w | \mu) = \sum_{k, x y_q-1} \nu(k, x y_q-1) I_K : w(k : x y_q-1 | \nu),
\]
Therefore,
\[
I(K : X^w, Y^w) \leq \sum_{k, x y_q-1} \nu(k, x y_q-1) \tilde{I}(k : x y_q-1 | \nu)
= \sum_{k, x y_w} \mu(k, x y_w) \tilde{I}(k : x y_w | \mu)
= \sum_{k, x y_w} \mu(k, x y_w) \tilde{I}(k : x y_w | \mu)
+ \sum_{k, x y_w \in G} \mu(k, x y_w) \tilde{I}(k : x y_w | \mu)
\leq \gamma + \phi \cdot \log \#K + \epsilon \cdot \#K
= \gamma + (\phi + \epsilon) \#K.
\]

4.3 Instance secrecy of Shamir’s scheme

The Shamir $(q, w)$-threshold scheme (see [Sha79]) in $\mathbb{Z}_p$, with $p \geq w + 1$ is constituted by two phases:

- **Initialization phase** $D$ publicly chooses $w$ distinct, non-zero elements of $\mathbb{Z}_p$, denoted by $x_i$, $1 \leq i \leq w$. For $1 \leq i \leq w$, $D$ gives the value $x_i$ to $P_i$.

- **Share distribution** Suppose $D$ wants to share a key $K \in \mathbb{Z}_p$. $D$ secretly chooses independently at random $q - 1$ elements of $\mathbb{Z}_p$, $a_1, \ldots, a_{q-1}$ and constructs a random polynomial $a(x) = K + \sum_{j=1}^{q-1} a_j x^j \mod p$, where $a(x) \in \mathbb{Z}_p[x]$ of degree at most $q - 1$.

- For $1 \leq i \leq w$, $D$ computes the secret share $y_i = a(x_i)$ and gives it to participant $P_i$.

For $1 \leq i \leq w$, every participant $P_i$ obtains a point $(x_i, y_i)$ on this polynomial where all the coefficients $a_0, \ldots, a_{q-1}$ are unknown elements of $\mathbb{Z}_p$ and $a_0 = K$ is the key. A set $B \subseteq P, B = \{P_{i_1}, 1 \leq i_j \leq w, 1 \leq j \leq q \}$ can reconstruct the key by means of polynomial interpolation like the Lagrange formula, which is an explicit formula to recover $a(x)$ given $q$ points $(x_{i_1}, y_{i_1}), \ldots, (x_{i_q}, y_{i_q})$ on the polynomial.

We identify the secure instances of Shamir’s scheme to be the ones where the key and the shares are independent according to Kolmogorov complexity.

**Lemma 1** Let $(k, x y_w)$ be an instance of the Shamir secret sharing scheme. For any set $B \subseteq [w]$ with $|B| = q - 1$, if $K(k, x y_B^{q-1} | \mu) \geq K(k | \mu) + |x y_B^{q-1}| - \alpha$ then $I(k : x y_B^{q-1} | \mu) \leq \alpha + O(1)$.

**Proof:** By assumption,
\[
K(k, x y_B^{q-1} | \mu) \geq K(k | \mu) + |x y_B^{q-1}| - \alpha,
\]
and symmetry of information gives that
\[ K(k, xy_B^{q-1}|\mu) = K(xy_B^{q-1}|\mu) + K(k|xy_B^{q-1}, K(xy_B^{q-1}|\mu), \mu) \]
\[ \leq |xy_B^{q-1}| + K(k|xy_B^{q-1}, K(xy_B^{q-1}|\mu), \mu) + O(1). \]
Therefore,
\[ K(k|\mu) + |xy_B^{q-1}| - \alpha - O(1) \leq K(k|xy_B^{q-1}, K(xy_B^{q-1}|\mu), \mu) + |xy_B^{q-1}| \]
\[ \Leftrightarrow K(k|xy_B^{q-1}, K(xy_B^{q-1}|\mu), \mu) \geq K(k|\mu) - |xy_B^{q-1}| - \alpha - O(1) \]
\[ \Leftrightarrow I(k : xy_B^{q-1}|\mu) \leq \alpha + O(1) \]

For Shamir’s scheme, we can infer information theoretic security from instance security, as follows.

**Theorem 23** Under the uniform distribution over the random shares and a computable distribution over the secret, Shamir’s secret sharing scheme is \((\log \log p + 1)\) secure in the information theoretic sense.

**Proof:** For a given instance \((k, xy_B)\), and any \(xy_B^{q-1}\) arrangement derived from \(xy_B\), \(K(k, xy_B) \leq K(k, xy_B^{q-1}) + |x_{w-q+1}|\) where \(x_{w-q+1} = (x_1, x_2, \ldots, x_w) | ([w] \setminus B)\), that is, the public shares of all users not present in \(B\). This is because if we are given the description of \(q-1\) private shares and the secret \(k\) we can recover the secret polynomial and from there, using the remaining public values, compute all the missing private shares.

Then,
\[ K(k, xy_B|\mu) \leq \min_{B \subseteq [w], |B| = q-1} K(k, xy_B^{q-1}|\mu) + |x_{w-q+1}| \]
This means that if \(K(k, xy_B|\mu) \geq K(k|\mu) + |xy_B^{q-1}| + |x_{w-q+1}| - \alpha\), then for all arrangements \(xy_B^{q-1}\) of \(q-1\) users made from \((k, xy_B)\)
\[ K(k|xy_B^{q-1}, \mu) \geq K(k|\mu) + |xy_B^{q-1}| + |x_{w-q+1}| - \alpha - |x_{w-q+1}| \]
\[ \Leftrightarrow K(k|xy_B^{q-1}, \mu) \geq K(k|\mu) + |xy_B^{q-1}| - \alpha \]
which implies, by Theorem 1, \(I(k : xy_B^{q-1}|\mu) \leq \alpha + O(1)\). Then, by definition, this instance will be \((\alpha, 0)\) secure.

Using \(K(k, xy_B|\mu) = K(k|\mu) + K(xy_B|k, K(k|\mu), \mu)\), the probability that \((k, xy_B)\) satisfies the above condition is:
\[
\Pr_{(k, xy_B)}[K(k, xy_B) \geq K(k|\mu) + |xy_B^{q-1}| + |x_{w-q+1}| - \alpha] \\
= \Pr_{(k, xy_B)}[K(xy_B|k, K(k|\mu), \mu) \geq |xy_B^{q-1}| + |x_{w-q+1}| - \alpha] \\
= \sum_{k} \mu_k(k) \sum_{xy_B \in \mathcal{W}} \mathcal{U}_w(xy_B)
\]
for \(\mathcal{W} = \{xy_B : K(xy_B|k, K(k|\mu), \mu) \geq |xy_B^{q-1}| + |x_{w-q+1}| - \alpha\}\)

In the Shamir scheme, the key and the public shares are all drawn independently from the same alphabet \(\mathcal{K}\). Also, by construction, any \(q-1\) private shares are also independent. So, a whole instance may be coded
by a string with just \((w + q - 1) \log p\) bits. Then, \(|xy_G^{q-1}| = 2(q - 1) \log p\), \(|x_{w-q+1}| = (w - 1 + q) \log p\) and \(|xy^w| = (w + q - 1) \log p\).

Since \(k\) is fixed, the conditional in the inner summation is fixed and so we can apply Theorem 4, item 4, to find there is at least a fraction \(1 - \frac{2(2(q-1)+(w-1)+q+1)) \log p - \alpha}{2(q-1)+w+1} \log p \) of secure instances.

Finally, let \(\alpha = \log \log p\) and apply Theorem 22 with \(\epsilon = \frac{1}{p \log p}\), \(\gamma = \log \log p\) and \(\phi = 0\). Then, the system has security \(\log \log p + 1\).

\[\square\]

5 Unconditional security of authentication codes without Secrecy

This section studies authentication codes. We follow the notation in [Sti91] to some extent. An authentication code is a four-tuple \((S, A, K, e)\), where \(S\) is a finite set of possible source states, \(A\) is a finite set of possible authentication tags and \(K\) is a finite set of possible keys. For each \(k \in K\), there is an authentication rule \(e_k : S \to A\) The message set is defined to be \(M = S \times A\). We consider only systems where each pair key / source state defines exactly one coded message.

There are two different types of attack by the opponent:

- **Impersonation**: The opponent sends a forged message \((s, a)\). The probability of success of this attack is denoted by \(P_i\).

- **Substitution**: The opponent replaces a valid message \((s, a)\) with a forgery \((s', a')\). The probability of success of this attack is denoted by \(P_s\).

5.1 Information theoretic security

We recall the results in the literature for the lower bounds on the opponent’s chances of success.

The probability that the recipient will accept \((s, a) \in S \times A\) as authentic is

\[
\text{payoff}(s, a) = \text{prob}_K(a = e_k(s))
\]

We define \(P_i = \max\{\text{payoff}(s, a) : s \in S, a \in A\}\)

**Theorem 24** ([S85]) For any authentication code \((S, A, K, e)\) without splitting \(P_i \geq 2^{-h(K)+h(K|M)} = 2^{-h(A|S)}\).

In the substitution case, the attacker knows a legitimate message \(m = (s, a)\). The probability that the recipient accepts the forgery \((s', a')\) is

\[
\text{payoff}(s', a', m) = \frac{\sum_{k \in K : a = e_k(s) \text{ and } a' = e_k(s')} p(k)}{\sum_{k \in K : a = e_k(s)} p(k)} = p(a'|s', m)
\]

As before, define \(P_s = \max\{\text{payoff}(s', a', m) : s' \in S, a' \in A, m \in M\}\).

From here we can easily show the following.

**Corollary 25** For an authentication code \((S, A, K, e)\) without splitting \(P_s \geq 2^{-h(A|S)}\).

**Theorem 26** ([B84]) For any authentication code \((S, A, K, e)\) without splitting \(P_s \geq 2^{-h(K|M)}\).
Note that $H(K|M) \geq H(A|S, M)$ and so the first lower bound implies the second.

An authentication code is said to have perfect security if the previous bounds are attained, i.e., $P_i = 2^{-H(A|S)}$, and $P_s = 2^{-H(A|S,M)}$.

We generalise the notion of security in the following definition:

**Definition 27** An authentication code $(S, A, K, e)$ has $(\delta, \delta')$ security if

1. $\log P_i \leq -H(A|S) + \delta$
2. $\log P_s \leq -H(A|S, M) + \delta'$

### 5.2 Instance security against impersonation

We define the security of an individual instance $(s, a)$ of an authentication scheme.

**Definition 28** Let $(S, A, K, e)$ be an authentication code without splitting and $\mu$ a distribution over $S \times K$.

- an instance $(s, a)$ is $\gamma$ secure against impersonation if $K(a|s, K(s|\mu), \mu) \geq \log(\#A) - \gamma$.
- an instance $(a, s, m)$ is $\gamma'$ secure against substitution if $K(a|s, m, K(s, m|\mu), \mu) \geq \log(\#A) - \gamma'$.

The following theorem allows us to relate the deception probabilities to Kolmogorov based security of instances.

**Theorem 29** For any authentication code $(S, A, K, e)$ without splitting, for any independent variables $S, K$ over $S, K$ with computable distribution $\mu$ and any large enough polynomial time bound $t$,

1. for any instance $(a, s)$ of the authentication code,

$$2^{-\max_{a,s} K^t(a|s, K(s|\mu), \mu)} \leq P_i \leq 2^{-\min_{a,s} K^t(a|s, K(s|\mu), \mu)}.$$

2. for any instance $(a, s, m)$ of the authentication code,

$$2^{-\max_{a,s,m} K^t(a|s,m, K(s,m|\mu), \mu)} \leq P_s \leq 2^{-\min_{a,s,m} K^t(a|s,m, K(s,m|\mu), \mu)}.$$

**Proof:** For the first statement,

$$\max_{a,s} K^t(a|s, K(s|\mu), \mu) \geq \sum_{a,s} p(a,s) K^t(a|s, K(s|\mu), \mu)$$

$$\geq H(A|S)$$

$$\geq \log(1/P_i)$$

$$\geq \min_{a,s} K^t(a|s, K(s|\mu), \mu)$$

The first inequality is trivial; the second follows from Theorem 9. The third is Theorem 24. Finally, the last inequality follows by using the Shannon-Fano code, which encodes a source $\{(x, p(x))\}$ with codewords of length $\log 1/p(x)$. This encoding can be carried out in polynomial time if the distribution $\mu$ is given.
Similarly, for the second statement (using Theorem 25 instead of Theorem 24)

\[
\max_{a,s,m,\mu} K^t(a|s, m, K(s, m|\mu), \mu) \geq \sum_{a,s,m,\mu} p(a, s, m) K^t(a|s, m, K(s, m|\mu), \mu) \\
\geq H(A|S, M) \\
\geq \log(1/P_s) \\
\geq \min_{a,s,\mu} K^t(a|s, m, K(s, m|\mu), \mu).
\]

\[\square\]

**Corollary 30** For any authentication code \((S, A, K, e)\) without splitting,

1. if all instances \((a, s)\) are \(\gamma\)-secure against an impersonation attack;
2. if all instances \((a, s, m)\) are \(\gamma'\)-secure against a substitution attack;

then the authentication code is \((\gamma, \gamma')\)-secure in the information theoretic sense.

## 6 Conclusion

By the close relation between information theory and Kolmogorov complexity, we have shown that there is also a very deep relation between Kolmogorov complexity and cryptography. Shannon’s entropy can almost be replaced by Kolmogorov complexity in the most important definitions of perfect secrecy of a private key cipher system, with the advantage that this gives us a notion of security of individual instances, instead of having a statistical notion.

We have only studied information theoretic cryptosystems in this paper, and many problems remain to be studied. The practical implications of the security of instances remains to be explored. However, we expect that the most promising extension of this work is to study computational models of security, such as in public-key cryptosystems. We expect that time bounded Kolmogorov complexity, and notions such as instance complexity \([OKSW94]\], will be the right technical tools to achieve this.
References


