JASS'05

Information-Theoretic Cryptography

Hermann Gruber

TU München

Information theory

- Counts among the foundations of computer science
- Pioneered by Claude Shannon
- Important for data compression, error-free transimission, and . . .

Information theory

- Counts among the foundations of computer science
- Pioneered by Claude Shannon
- Important for data compression, error-free transimission, and . . .

Cryptography.

Claude E. Shannon (1916-2001)

Most outstanding results of his work:

- brought Boolean algebra into circuit design
- introduced a mathematical theory of communication
- proved Nyquist's Sampling Theorem
- ...
- Most important for us here:
  first rigorous analysis of cryptosystems

(source: http://en.wikipedia.org)

Cryptosystems

Usually:

- Alfons and Boris secretly agree about a key k
- Alfons encrypts $T_k(m) = c$, sends it to Boris
- Boris decrypts $T_k^{-1}(c) = m$
- Ivan (the Terrible) intercepting c, tries to figure out m (or, worse, k)

In Shannon's view (Shannon 1949):

- Alfons is a statistical message source
- The key choice is a statistical information source, transmitted over a secure channel
- Ivan knows a priori probabilities for
  - m (natural language)
  - and k (habits of key choice)
- after intercepting c: a posteriori probabilities for m and k
- Ivan has unbounded time and computational power (!)
- Kerckhoffs' principle: (Kerckhoffs 1883, Shannon 1949) Ivan knows the encryption mechanism.

Can he gain statistical information about m from c?

Perfect Secrecy

Definition.(Shannon 1949)
A cryptosystem with probability distributions on message space M and keyspace K is said to be perfectly secret, if for all ciphertext messages c and all messages m holds

$$Pr[m \mid c] = Pr[m]$$

Example: One-Time Pad

aka Vernam-Cipher (Gilbert Vernam, 1926, patented 1919)

- $M = K = C = \{0,1\}^n$
- keys are chosen equiprobable
- encryption/decryption: bitwise modulo-2-addition of key and message
- key is only used once.

(Not that the key is as long as the message.) Can we prove that this system is perfectly secure?

Toolbox.

Ivan intercepts c and wants to know a posteriori (conditional) distribution on M.

Bayes' theorem.

If $P[C = c] > 0$, then

$$P[M = m \mid C = c] = \frac{P[C = c \mid M = m]P[M = m]}{P[C = c]}$$

C and M are independent iff
$P[M = m \mid C = c] = P[M = m]$.

Toolbox (cont'd).

Set of possible keys for cipher c:

$K(c) = \{k \in K \mid \exists m \in M : T_k(m) = c\}$

Set of possible keys for m and c:

$K(c, m) = \{k \in K \mid T_k(m) = c\}$.

Toolbox (cont'd).

Set of possible keys for cipher c:

$K(c) = \{k \in K \mid \exists m \in M : T_k(m) = c\}$

Set of possible keys for m and c:

$K(c,m) = \{k \in K \mid T_k(m) = c\}$.

Then

$$P[C = c] = \sum_{k \in K(c)} P[K = k] P[M = T_k^{-1}(c)]$$

and

$$P[C = c \mid M = m] = \sum_{k \in K(c,m)} P[K = k]$$

Toolbox (cont'd).

Set of possible keys for cipher c:

$K(c) = \{k \in K \mid \exists m \in M : T_k(m) = c\}$

Set of possible keys for m and c:

$K(c, m) = \{k \in K \mid T_k(m) = c\}$.

Then

$$P[C = c] = \sum_{k \in K(c)} P[K = k] P[M = T_k^{-1}(c)]$$

and

$$P[C = c \mid M = m] = \sum_{k \in K(c,m)} P[K = k]$$

... into Bayes' formula $\Rightarrow P[M = m \mid C = c]$.

Return to One-time Pad.

We have to show $P[M = m \mid C = c] = P[M = m]$

For every k, we have $P[K = k] = \left(\frac{1}{2}\right)^n$. So

$$P[C = c] = \frac{1}{2}^n \sum_{k \in K(c)} P[M = T_k^{-1}(c)]$$

Return to One-time Pad.

We have to show $P[M = m \mid C = c] = P[M = m]$

For every k, we have $P[K = k] = \left(\frac{1}{2}\right)^n$. So

$$P[C = c] = \frac{1}{2}^n \sum_{k \in K(c)} P[M = T_k^{-1}(c)]$$

For every pair $\langle m, c \rangle$, there is a unique key $K(c, m) = \{k\}$, so

$$\sum_{k \in K(c)} P[M = T_k^{-1}(c)] = \sum m \in M P[M = m] = 1$$

Return to One-time Pad.

We have to show $P[M = m \mid C = c] = P[M = m]$

For every k, we have $P[K = k] = \left(\frac{1}{2}\right)^n$. So

$$P[C = c] = \frac{1}{2}^n \sum_{k \in K(c)} P[M = T_k^{-1}(c)]$$

For every pair $\langle m, c\rangle$, there is a unique key $K(c, m) = \{k\}$, so

$$\sum_{k \in K(c)} P[M = T_k^{-1}(c)] = \sum m \in M P[M = m] = 1$$

. . . and $P[C = c] = \left(\frac{1}{2}\right)^n$.

Return to One-time Pad(cont'd).

Assume $c = T_k(m)$. Then

$$P[C = c \mid M = m] = P[K = k] = \left(\frac{1}{2}\right)^n$$

Return to One-time Pad(cont'd).

Assume $c = T_k(m)$. Then

$P[C = c \mid M = m] = P[K = k] = \left(\frac{1}{2}\right)^n$

Putting these results into Bayes' formula yields

$$P[M = m \mid C = c] = \frac{\left(\frac{1}{2}\right)^n P[M = m]}{\left(\frac{1}{2}\right)^n}$$

Return to One-time Pad(cont'd).

Assume $c = T_k(m)$. Then

$P[C = c \mid M = m] = P[K = k] = \left(\frac{1}{2}\right)^n$

Putting these results into Bayes' formula yields

$$P[M = m \mid C = c] = \frac{\left(\frac{1}{2}\right)^n P[M = m]}{\left(\frac{1}{2}\right)^n}$$

and we are done.

Characterization of Perfect Secrecy Systems.

With little more effort, one can show:

Perfect Secrecy Theorem (Shannon 1949)

A cryptosystem provides perfect secrecy if and only if

- $|M| = |C| = |K|$
- every key is used with equal probability $1/|K|$,
- and for every message-cipher-pair $\langle m, c\rangle$, there is a unique key k with $c = T_k(m)$.

(Proof can be found in Stinson 2002.)

Consequences.

- Perfect Secrecy often impractical: key needs to be as long as the message
  Ways around:
- use of pseudo-random generators for Vernam cipher (e.g. DES in OFB mode) (...but NO perfect secrecy!)
- different notion of secrecy: prove computational hardness of code breaking
- Vernam cipher nevertheless in use for critical missions (politics, military)

More of Shannon's ideas

- What if we use the same key more than once?
- Analysis again due to Shannon, using entropy.
- entropy H(X) measures the average degree of uncertainity of a random variable X.

Entropy

Definition. Entropy.

Let X be a random variable taking values 1,. . . ,n

$$H(X) = -\sum_{i=1}^{n} P[X = i] log_2 P[X = i]$$

Conditional Entropy and Key Equivocation.

Let Y be another random variables, taking values 1,. . . ,m

The conditional entropy $H(X \mid Y)$ is

$$H(X \mid Y) = \sum_{j=1}^{m} p(Y = j) H(X \mid Y = j)$$

Conditional entropy measures the average uncertainity about X given observations of the variable Y.

Key Equivocation.

Using conditional entropy for cryptosystem analysis:
How much average uncertainty remains about the key remains provided we know the ciphertext?

Key Equivocation.

Using conditional entropy for cryptosystem analysis:
How much average uncertainty remains about the key remains provided we know the ciphertext?

$H(K \mid C)$ is called the key equivocation.

Key Equivocation (cont'd).

Shannon found that

$$H(K \mid C) = H(M) + H(K) - H(C)$$

In particular, for perfect secrecy systems, we have
$H(K \mid C) = H(K)$.
That is, uncertainty about the key does not decrease with knowledge of the ciphertext. (Shannon 1949)

Conclusion

What we have encountered:

- Vernam Cipher
- Perfect secrecy
- Drawbacks in perfect secrecy
- Tools for analyzing “imperfect” systems

References/Further Reading

- Shannon, Claude E. : Communication Theory of Secrecy Systems,Bell System Technical Journal, vol.28-4, page 656-715, 1949

- Smart, Nigel; Lee, John Malone: Introduction to Cryptography (COMS30124), Lecture notes. Available online at www.cs.bris.ac.uk

- Stinson,Douglas R. : Cryptography. Theory and Practice. 2002