Attainable Unconditional Security for Shared-Key Cryptosystems

Adolf Středa

Škola v přírodě Katedry algebry; April 4, 2019

Motivation

- *Perfect secrecy* is impractical
- Computational security has its flaws

Entropy

Definition

Given two random variables X, Y we define the following functions:

Entropy

$$H(X) = -\sum_{x \in X} Pr(X = x) \log_2 Pr(X = x)$$

Mutual information

$$I(X;Y) = \sum_{x \in X} \sum_{y \in Y} Pr(X = x, Y = y) \log_2 \left(\frac{Pr(X = x, Y = y)}{Pr(X = x) Pr(Y = y)} \right)$$

Entropy

Definition

Given two random variables X, Y we define the following functions:

Joint entropy

$$H(X,Y) = -\sum_{x \in X} \sum_{y \in Y} Pr(X = x, Y = y) \log_2 Pr(X = x, Y = y)$$

Conditional entropy

$$H(X|Y) = H(X,Y) - H(Y)$$

Cryptosystem

Definition

A (shared-key) cryptosystem is a 3-tuple $(\mathcal{M}, \mathcal{K}, enc)$ where:

- $\mathcal{M}$ is a finite set of possible messages (message space)
- $\mathcal{K}$ is a finite set of possible keys (key space)
- the encoder enc is a function $\mathcal{M} \times \mathcal{K} \to \mathcal{C}$ to some space $\mathcal{C}$ such that $\forall k \in \mathcal{K} : enc(\_, k)$ is injective.

Examples

AES: $\mathcal{M} = \{0,1\}^{128} = \mathcal{C}, \mathcal{K} = \{0,1\}^{128 \text{ or } 192 \text{ or } 256}$,
the encryption function for a given key is a bijection.

Cryptosystem 2

Definition

Let $\mathcal{C} = \{c | \exists m \in \mathcal{M} \exists k \in \mathcal{K} : c = enc(m, k)\}$ be the ciphertext space.

Definition

Let the decoder dec be the function $\mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M}$ such that $dec(enc(m, k), k) = m$.

The existence of dec is guaranteed by the injectivity of enc.

Perfect secrecy

Let $M/C/K$ be a random variable on the support set $\mathcal{M}/\mathcal{C}/\mathcal{K}$.
We assume that M and K are independent, i.e.
$H(M, K) = H(M) + H(K)$.

Definition

A cryptosystem attains perfect secrect iff $H(M) = H(M|C)$.

As the name mutual information suggests the following equivalence holds: $H(M) = H(M|C) \Leftrightarrow I(M; C) = 0$.

Lemma

Perfect secrecy implies $|\mathcal{K}| \geq |\mathcal{M}|$.

Wait. . . isn't that a little bit impractical?

- Message equivocation $H(M|C)$

- Message equivocation $H(M|C)$
- $I(M;C) = H(M) - H(M|C)$, i.e. perfect secrecy implies $H(M|C) = H(M)$

- Message equivocation $H(M|C)$
- $I(M;C) = H(M) - H(M|C)$, i.e. perfect secrecy implies $H(M|C) = H(M)$
- Shannon: $H(K) \geq H(M)$ necessary condition for perfect secrecy
- $H(M|C) \leq min(H(M), H(K))$

- Message equivocation $H(M|C)$
- $I(M;C) = H(M) - H(M|C)$, i.e. perfect secrecy implies $H(M|C) = H(M)$
- Shannon: $H(K) \geq H(M)$ necessary condition for perfect secrecy
- $H(M|C) \leq min(H(M), H(K))$
- Theoretical maximal equivocation achieved when corresponding to $min(H(M), H(K))$

Max-Equivocation

Definition

A cryptosystem achieves max-equivocation iff

$$H(M|C) = min(H(M), H(K))$$

We could define key-equivocation similarly for $H(K|C)$.

Definition

A function $f : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$ is semi-injective on $\mathcal{B}$ iff it holds that $\forall a \in \mathcal{A} \forall b_i, b_j \in \mathcal{B} : f(a, b_i) = f(a, b_j) \Leftrightarrow b_i = b_j$.

Lemma

f semi-injective on $\mathcal{A}$ then $|f(\mathcal{A}, \mathcal{B})| \geq |\mathcal{A}|$. f semi-injective on both $\mathcal{A}, \mathcal{B}$ then $|f(\mathcal{A}, \mathcal{B})| \geq max(|\mathcal{A}|, |\mathcal{B}|)$.

Lemma

f semi-injective on $\mathcal{A}$, A r.v. on $\mathcal{A}$, C r.v. on $\mathcal{C}$ then $H(A) \leq H(C)$.

Proof.

$|f(\mathcal{A}, \mathcal{B})| = |\mathcal{A}| \Rightarrow \exists c \in f(\mathcal{A}, \mathcal{B})$ corresponding to each $a \in \mathcal{A}$. $|f(\mathcal{A}, \mathcal{B})| > |\mathcal{A}| \Rightarrow \exists c_i \neq c_j : f(a, b_x) = c_i, f(a, b_y) = c_j$. This increases entropy, i.e. $H(A) \leq H(C)$. □

Semi-injectivity in cryptosystems

Let $(\mathcal{M}, \mathcal{K}, enc)$ be a cryptosystem.

Lemma

$$max(H(M), H(K)) \leq H(C) \leq H(M) + H(K)$$

Lemma

$$H(C|M) = H(K)$$

Utilising these two lemmata, we set bounds for equivocation

Theorem

$$0 \leq H(M|C) \leq min(H(M), H(K))$$

Corollary

$H(C) = max(H(M), H(K)) \Leftrightarrow H(M|C) = min(H(M), H(K))$

Proof.

$H(M|C) = H(C|M) + H(M) - H(C) = H(K) + H(M) - H(C)$
that is $H(M|C)$ *maximal iff* $H(C)$ *minimal* □

Key-reuse

Let $\vec{m} \in \mathcal{M}^n$ be a vector of messages, similarly $\vec{k} \in \mathcal{K}^n$ vector of keys. Since $H(\vec{M}) = nH(M)$ (m_i are independent), the equivocation of the repeated transmission is:

$$H(\vec{M}, \vec{C}) = H(\vec{C}|\vec{M}) + H(\vec{M}) - H(\vec{C})$$

$$= H(\vec{C}|\vec{M}) + nH(M) - H(\vec{C}) = H(\vec{K}) + nH(M) - H(\vec{C})$$

Independent keys: $H(\vec{K}) = nH(K)$; same key: $H(\vec{K}) = H(K)$.

Theorem

$H(M|C) = H(K|C)$

Using this observation and the theorem we may show that equivocation does not differ between encrypting using parts of the total shared key or repeatedly using the shared key.

Bounds on Key Equivocation

Theorem

$0 \leq H(K|C) \leq min(H(K), H(M))$

Theorem

$I(M, K; C) \geq |H(K) - H(M)|$

This theorem states that the information leakage about the message and the key is minimal when they have the same size. Moreover, it shows that using a key with entropy than the message is unnecessary.

Lemma

If $H(K) > H(M)$ and perfect secrecy holds then $H(M)$ bits of the key are used to protect the message with perfect secrecy and the rest is leaked to the attacker.

Q&A