Thm. Equivalent notions of PERFECT SECRECY:

(i) The above definition.

(ii) M and C are INDEPENDENT.

(iii) $\forall\ m, m' \in \mathcal{M}$, $\forall\ c \in \mathcal{C}$

$$Pr[Enc(K, m) = c] = Pr[Enc(K, m') = c]$$

Proof. (i) $\Rightarrow$ (iii)

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

$$= \frac{Pr[M = m \wedge C = c]}{Pr[C = c]}$$

$$\Rightarrow \Pr[M = m \wedge C = c] = \Pr[M = m] \cdot \Pr[C = c].$$

(2) $\Rightarrow$ (3) Fix M, $m \in \mathcal{M}$, $c \in \mathcal{C}$:

$$\Pr[\mathrm{Enc}(K, \overset{m'}{m}) = c] = \qquad m' \in \mathcal{M}$$

$$\Pr[\mathrm{Enc}(K, M) = c \mid M = \overset{m'}{m}]$$

$$= \Pr[C = c \mid M = \overset{m'}{m}]$$

$$= \Pr[C = c]$$

✓

$(1) \wedge (1') \Rightarrow (1)$. Take any $c \in \mathcal{C}$

$$\Pr[C = c] = \sum_{m'} \Pr[C = c \wedge M = m']$$

$$= \sum_{m'} \Pr[C = c \mid M = m'] \cdot \Pr[M = m']$$

$$= \sum_{m'} \Pr[Enc(K, M) = c \mid M = m'] \cdot \Pr[M = m']$$

$$= \sum_{m'} \Pr[Enc(K, m') = c] \cdot \Pr[M = m']$$

$$= \sum_{m'} \Pr[Enc(K, m) = c] \cdot \Pr[M = m']$$

$$= \Pr[Enc(K, m) = c] \cdot 1$$

$$= \Pr[Enc(K, M) = c \mid M = m]$$

$$= \Pr[C = c \mid M = m].$$

$$\Rightarrow \Pr[C = c] = \Pr[C = c \mid M = m]$$

Apply Bayes:

$$\Pr[M = m \mid C = c] \cdot \Pr[C = c] = \Pr[M = m \wedge C = c]$$

$$\Rightarrow \Pr[M = m] = \frac{\Pr[M = m \mid C = c] \cdot \Pr[C = c]}{\Pr[C = c \mid M = m]}$$

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

$$\Rightarrow \Pr[M=m] = \Pr[M=m \mid C=c]$$

Application: One-Time pad is perfectly secure.

$$\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$$

$$Enc(k, m) = c = k \oplus m$$

$$Dec(k, c) = c \oplus k = k \oplus m \oplus k = m$$

Cor. $\Pi = (Enc, Dec)$ above is perfectly secret.

Proof. Fix any $m \in \mathcal{M}$, $c \in \mathcal{C}$:

$$\Pr[Enc(K, m) = c] =$$

$$= \Pr[K \oplus m = c]$$

$$= \Pr[K = c \oplus m] = 2^{-n}$$

$$= \Pr[K = c \oplus m']$$

$$= \Pr[Enc(K, m') = c]$$

Drawbacks: - One-time notion (only one c)

$$- |K| = |M|$$

Two-Time: $c_1 = K \oplus m_1$

$$c_2 = K \oplus m_2$$

$$c_1 \oplus c_2 = m_1 \oplus m_2$$

THM. In any PERFECTLY SECRET SKS $\Pi = (Enc, Dec)$, we have $|K| \geq |M|$.

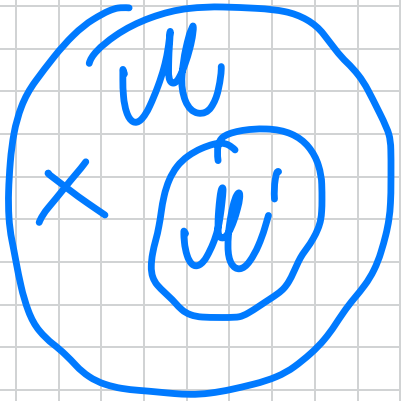
Proof. Take M to be UNIFORM over $\mathcal{M}$.
Take any $c \in \mathcal{C}$ s.t. $Pr[C = c] > 0$.

Consider: → ALL WAYS TO DECRYPT c

$$M' = \{ Dec(k, c) : k \in K \}$$

Assume $|K| < |M|$. We will show PERFECT SECRECY does not hold.

Observe: $|M'| \leq |K| < |M|$



There exists $m \in M \setminus M'$

But now:

$$Pr[M = m \mid C = c] = 0$$

$$Pr[M = m] = 1/|M| \quad \blacksquare$$

PERFECT (STATISTICAL) AUTHENTICATION

DEF We say Tag has ε-STATISTICAL security if $\forall$ $m, m' \in \mathcal{M}$, $\forall$ $\tau, \tau' \in T$ $(m \neq m')$

$$Pr[\, Tag(K, m') = \tau' \mid Tag(K, m) = \tau \,] \leq \varepsilon.$$

(e.g. $\varepsilon = 2^{-80}$)

NOTE: Not possible to get $\varepsilon = 0$.

Construction based on any PAIRWISE INDEPENDENT HASH FUNCTION.

DEF $\mathcal{H} = \{ h_k : \mathcal{M} \to \mathcal{T} \}$ is PAIRWISE INDEPENDENT if $\forall\, m, m' \in \mathcal{M}$, $m \neq m'$ then $(h_K(m), h_K(m'))$ is UNIFORM over $\mathcal{T}^2$ over choice of $K \in \mathcal{K}$.

Next time: — Tag $(K, m) = h_K(m)$ is $\frac{1}{|\mathcal{T}|}$-stat. secure.

→ $h_{a,b}(x) \equiv ax + b \mod p$

$(a, b) \in \mathbb{Z}_p^2$ is pairwise independent.