

# Does additional information *always* reduce anonymity?

---

Claudia Diaz, Carmela Troncoso and George Danezis

K.U.Leuven ESAT/COSIC

# Overview

- Anonymity: concept and metric
- Combination of several sources of information
  - The claim
  - The counterexample
  - The explanation
- Conclusions

# Anonymity – concept and metric

- “State of being not identifiable within a set of subjects, the *anonymity set*” [PHoo]
  - “Set of all possible subjects who might cause an action”
- Shannon *entropy*: measure of the uncertainty of a random variable
  - Increases with the number of possible values and the uniformity of the probability distribution
  - Proposed as anonymity metric [SDo2,DCSPo2], describes the uncertainty of the attacker on the identity of a user
  - Can be applied to mix traffic traces, or to user profiles (example later)

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

# Combining several sources of information- The claim

- “Let  $X$  and  $Y$  be probability distributions of the application layer and the network layer. One can measure anonymity  $H(X)$  and  $H(Y)$ . [T]he attacker could build a combined model by introducing the circumstances of communication as attributes in the application layer model. Due to the fact that **new information can only reduce the cardinality of the set of suspects** the resulting probability distribution gets more unequal, i.e., **entropy decreases.**” [CS06]
- Intuitively consistent with Shannon’s result on conditional entropy:  $H(Y|X) \leq H(Y)$

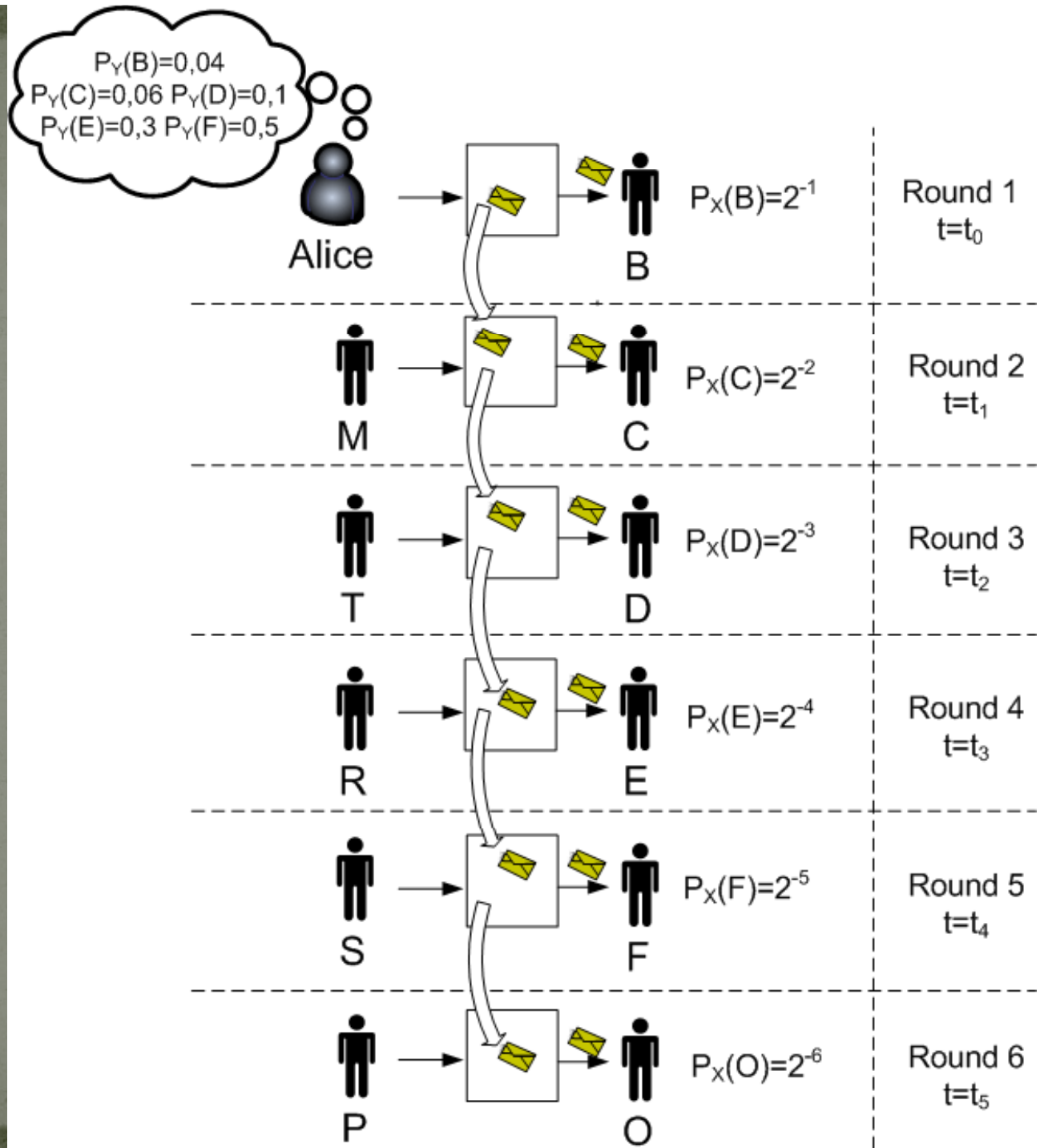
- $Y$  : Random variable describing Alice's sending profile

- $H(Y) = 1.78 \text{ bits}$

- Pool mix with threshold  $T=2$  and pool  $P=1$

- $X$  : Random variable describing communication trace observations:  $P_X(R_i)=2^{-i}$

- $H(X) = 2 \text{ bits}$



## Five possibilities for message $m$ :

1. Message was for Bob ( $P_Y(B)=0.04$ ) and it was immediately sent by the mix ( $P_X(1)=2^{-1}$ )
2. Message was for Charlie ( $P_Y(C)=0.06$ ) and it spent one round in the mix before being sent ( $P_X(2)=2^{-2}$ )
3. Message was for Dave ( $P_Y(D)=0.1$ ) and it spent two rounds in the mix before being sent ( $P_X(3)=2^{-3}$ )
4. Message was for Els ( $P_Y(E)=0.3$ ) and it spent three rounds in the mix before being sent ( $P_X(3)=2^{-4}$ )
5. Message was for Fred ( $P_Y(F)=0.5$ ) and it spent four rounds in the mix before being sent ( $P_X(4)=2^{-5}$ )

# Combining several sources of information- The (counter)example

- We define a random variable  $Z$  that combines both Alice's profile ( $Y$ ) and the communication trace ( $X$ )
  - $Z$  takes values  $\{z_i\} = \{B, C, D, E, F\}$

$$P_Z(z_i) = \frac{P_Y(y_i)P_X(i)}{\sum_j P_Y(y_j)P_X(j)}$$

$$P_Z(B)=0.25, P_Z(C)=0.18, P_Z(D)=0.15, P_Z(E)=0.23, P_Z(F)=0.19$$

$$H(Z) = 2.3 \text{ bits } (> H(X) = 2 \text{ bits } ; > H(Y) = 1.78 \text{ bits}) !!$$

# Relationship between attacker uncertainty and conditional entropy

$$H(Y | X) = -\sum_{i,j} \Pr(y_i, x_j) \log_2 \Pr(y_i | x_j)$$

$$\Pr(y_i, x_j) = \Pr(x_j) \Pr(y_i | x_j)$$

$$H(Y | X) = -\sum_j \Pr(x_j) \sum_i \Pr(y_i | x_j) \log_2 \Pr(y_i | x_j)$$

Given a trace  $x_j$ , the uncertainty of the attacker is given by the entropy  $H_j(Z)$ :  $H_j(Z) = -\sum_i \Pr(y_i | x_j) \log_2 \Pr(y_i | x_j)$

$$H(Y | X) = \sum_j \Pr(x_j) H_j(Z)$$

# Conclusions

- Using Shannon's entropy for computing the anonymity of either a profile or a communication trace is well understood
- BUT integrating several sources of information is not!
- As Shannon proves that  $H(Y|X) \leq H(Y)$ , some researchers believe that more information *must always* lead to a reduction of anonymity
- We have shown that this is not true for some concrete cases, and explained the relationship between “attacker uncertainty” and “conditional entropy”