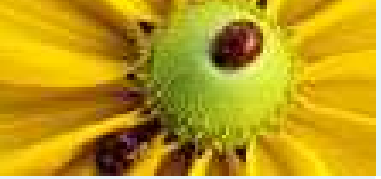
The Thermodynamic of Interference
COW19,
UCL May 2012

Pasquale Malacaria

Queen Mary University of London

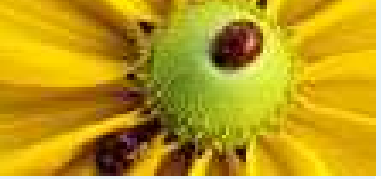
pm@eecs.qmul.ac.uk



A surprising connection

non-interference = perfect confidentiality

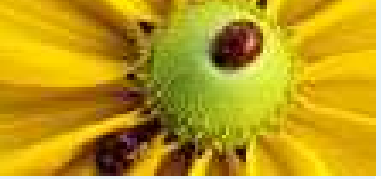
- What has a property (confidentiality) of a human artefact (software) in common with the fundamental laws of the physical world?



A surprising connection

non-interference = perfect confidentiality

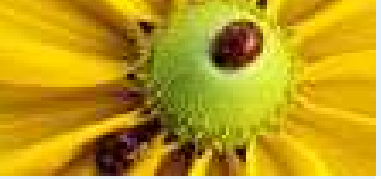
- What has a property (confidentiality) of a human artefact (software) in common with the fundamental laws of the physical world?
- Abstract of this talk:



A surprising connection

non-interference = perfect confidentiality

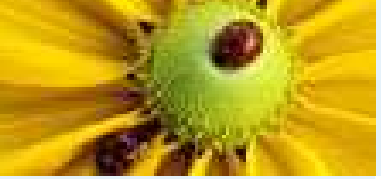
- What has a property (confidentiality) of a human artefact (software) in common with the fundamental laws of the physical world?
- Abstract of this talk:
- thermodynamics foundations of confidentiality



A surprising connection

non-interference = perfect confidentiality

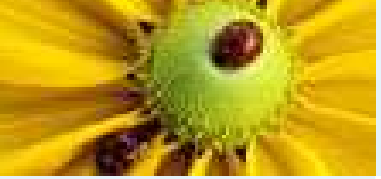
- What has a property (confidentiality) of a human artefact (software) in common with the fundamental laws of the physical world?
- Abstract of this talk:
- thermodynamics foundations of confidentiality
- Aim of this talk:



A surprising connection

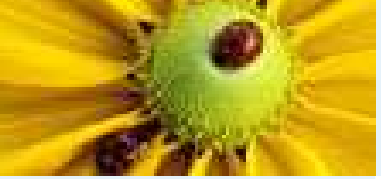
non-interference = perfect confidentiality

- What has a property (confidentiality) of a human artefact (software) in common with the fundamental laws of the physical world?
- Abstract of this talk:
- thermodynamics foundations of confidentiality
- Aim of this talk:
- hopefully to be thought provoking (apologies, not an engineering talk).



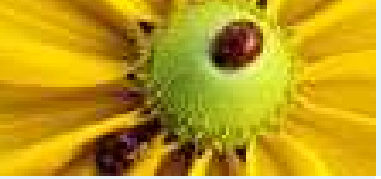
The problem and security model:

- An attacker has some a priori knowledge of the secret which is improved by observing the system



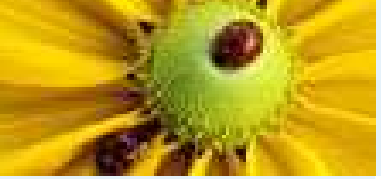
The problem and security model:

- An attacker has some a priori knowledge of the secret which is improved by observing the system
- measure this improvement: how much did the attacker gain from the observations?



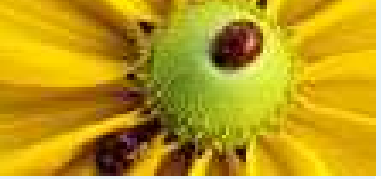
The problem and security model:

- An attacker has some a priori knowledge of the secret which is improved by observing the system
- measure this improvement: how much did the attacker gain from the observations?
  - **Example:**
    - an attacker steal your cash card; he has no idea about your pin (apriori probability to guess it 0.0001)
    - to randomly try a pin number at a cash machine will generate two possible observations:



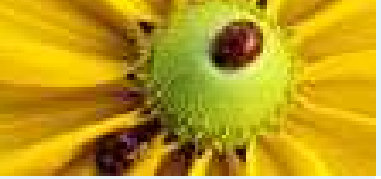
The problem and security model:

- An attacker has some a priori knowledge of the secret which is improved by observing the system
- measure this improvement: how much did the attacker gain from the observations?
  - **Example:**
    - an attacker steal your cash card; he has no idea about your pin (apriori probability to guess it 0.0001)
    - to randomly try a pin number at a cash machine will generate two possible observations:
  - the pin is accepted (with probability 0.0001),



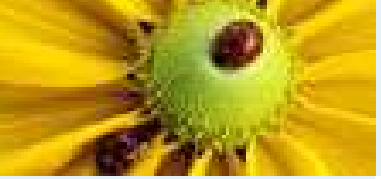
The problem and security model:

- An attacker has some a priori knowledge of the secret which is improved by observing the system
- measure this improvement: how much did the attacker gain from the observations?
  - **Example:**
    - an attacker steal your cash card; he has no idea about your pin (apriori probability to guess it 0.0001)
    - to randomly try a pin number at a cash machine will generate two possible observations:
  - the pin is accepted (with probability 0.0001),
  - the pin is rejected (with probability 0.9999)



The problem and security model:

- An attacker has some a priori knowledge of the secret which is improved by observing the system
- measure this improvement: how much did the attacker gain from the observations?
  - **Example:**
    - an attacker steal your cash card; he has no idea about your pin (apriori probability to guess it 0.0001)
    - to randomly try a pin number at a cash machine will generate two possible observations:
  - the pin is accepted (with probability 0.0001),
  - the pin is rejected (with probability 0.9999)
  - what has he learned?

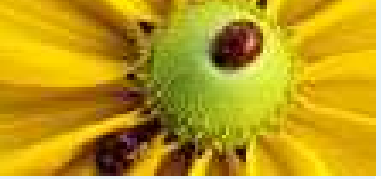


Quantitative analysis of confidentiality :

Given a function F measuring *knowledge* compute the difference of the measure F on the secret h before and after observing the system P

-

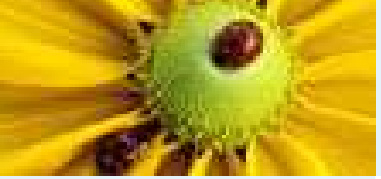
$$\Delta_F(P,h) = F(h) - F(h|P)$$



Quantitative analysis of confidentiality :

Given a function F measuring *knowledge* compute the difference of the measure F on the secret h before and after observing the system P

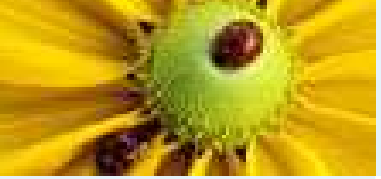
- $$\Delta_F(P, h) = F(h) - F(h|P)$$
- $F(h) =$ measure of the secret h before observations (a priori knowledge)



Quantitative analysis of confidentiality :

Given a function F measuring *knowledge* compute the difference of the measure F on the secret h before and after observing the system P

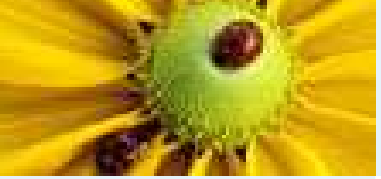
- $$\Delta_F(P, h) = F(h) - F(h|P)$$
- $F(h) =$ measure of the secret h before observations (a priori knowledge)
- $F(h|P)$ measure of the secret h given observations P (a posteriori knowledge)



Quantitative analysis of confidentiality :

$$\Delta_F(P,h) = F(h) - F(h|P)$$

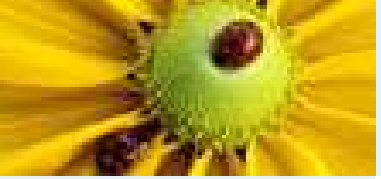
- What function F measuring *knowledge* to choose?



Quantitative analysis of confidentiality :

$$\Delta_F(P, h) = F(h) - F(h|P)$$

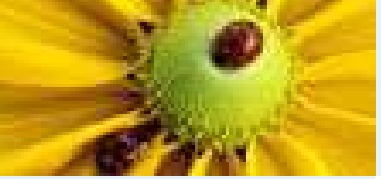
- What function F measuring *knowledge* to choose?
- see $F(h) - F(h|P)$ as the Attacker's reduction in uncertainty about the secret:



Quantitative analysis of confidentiality :

$$\Delta_F(P, h) = F(h) - F(h|P)$$

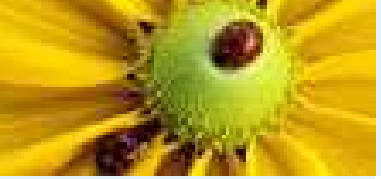
- What function F measuring *knowledge* to choose?
- see $F(h) - F(h|P)$ as the Attacker's reduction in uncertainty about the secret:
- $F(h) =$ initial Attacker's uncertainty about the secret h



Quantitative analysis of confidentiality :

$$\Delta_F(P, h) = F(h) - F(h|P)$$

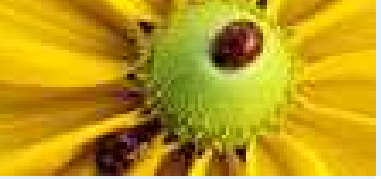
- What function F measuring *knowledge* to choose?
- see $F(h) - F(h|P)$ as the Attacker's reduction in uncertainty about the secret:
- $F(h) =$ initial Attacker's uncertainty about the secret h
- $F(h|P) =$ Attacker's remaining uncertainty about h given the observations



Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

$$\Delta_F(P, h) = F(h) - F(h|P)$$

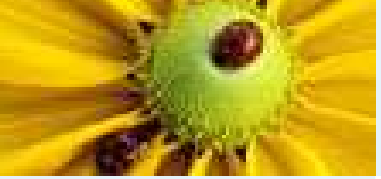


Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

$$\Delta_F(P, h) = F(h) - F(h|P)$$

- possible choices for $F, F(-|-)$ given by Shannon's information theory:

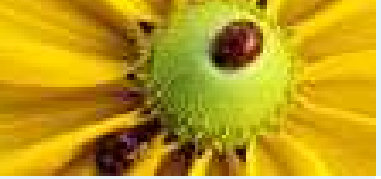


Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

$$\Delta_F(P,h) = F(h) - F(h|P)$$

- possible choices for $F, F(-|-)$ given by Shannon's information theory:
- $F(h) = H(h)$=initial uncertainty=entropy of secret h before observations= a priory information about h

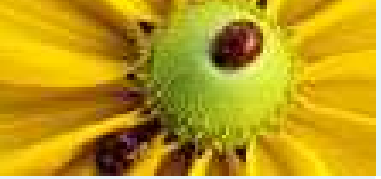


Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

$$\Delta_F(P,h) = F(h) - F(h|P)$$

- possible choices for $F, F(-|-)$ given by Shannon's information theory:
- $F(h) = H(h)$=initial uncertainty=entropy of secret h before observations= a priory information about h
- $F(h|P) = H(h|P)$=remaining uncertainty=entropy of secret h given observations= information about h given observations

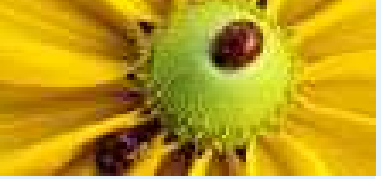


Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

$$\Delta_F(P,h) = F(h) - F(h|P)$$

- possible choices for $F, F(-|-)$ given by Shannon's information theory:
- $F(h) = H(h)$=initial uncertainty=entropy of secret h before observations= a priory information about h
- $F(h|P) = H(h|P)$=remaining uncertainty=entropy of secret h given observations= information about h given observations
- Δ_H (Cash machine,h)=0.00147

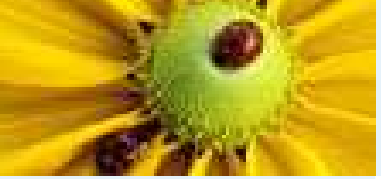


Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

$$\Delta_F(P,h) = F(h) - F(h|P)$$

- possible choices for $F, F(-|-)$ given by Shannon's information theory:
- $F(h) = H(h)$=initial uncertainty=entropy of secret h before observations= a priory information about h
- $F(h|P) = H(h|P)$=remaining uncertainty=entropy of secret h given observations= information about h given observations
- Δ_H (Cash machine,h)=0.00147
- Clark-Hunt-Malacaria 2002, inspired by Dennings, McLean, Gray



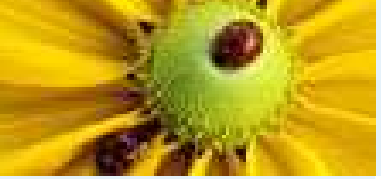
Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

■

$$\Delta_H(P,h) = H(h) - H(h|P)$$

(Notice $\Delta_H(P,h) \geq 0$)



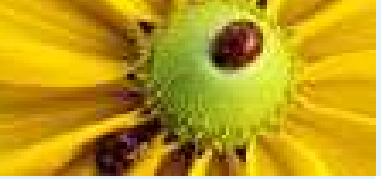
Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

$$\Delta_H(P,h) = H(h) - H(h|P)$$

(Notice $\Delta_H(P,h) \geq 0$)

- Easy to show that $\Delta_H(P,h) = 0$ iff the system leaks no information.

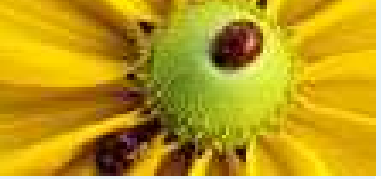


Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

- $$\Delta_H(P,h) = H(h) - H(h|P)$$

  (Notice $\Delta_H(P,h) \geq 0$)
- Easy to show that $\Delta_H(P,h) = 0$ iff the system leaks no information.
- hence $\Delta_H(P,h) = 0$ iff noninterference.

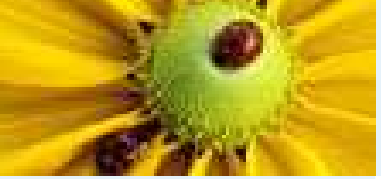


Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

- $$\Delta_H(P,h) = H(h) - H(h|P)$$

  (Notice $\Delta_H(P,h) \geq 0$)
- Easy to show that $\Delta_H(P,h) = 0$ iff the system leaks no information.
- hence $\Delta_H(P,h) = 0$ iff noninterference.
- But what does it mean when interference is positive?

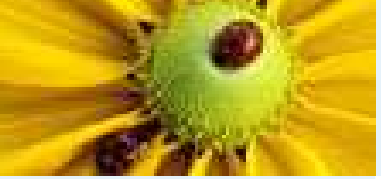


Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

- $$\Delta_H(P,h) = H(h) - H(h|P)$$

  (Notice $\Delta_H(P,h) \geq 0$)
- Easy to show that $\Delta_H(P,h) = 0$ iff the system leaks no information.
- hence $\Delta_H(P,h) = 0$ iff noninterference.
- But what does it mean when interference is positive?
- what does it mean $\Delta_H(P,h) = C > 0$

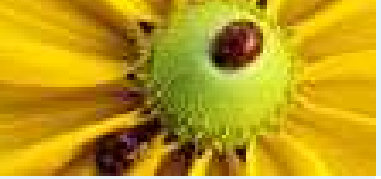


Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

- $$\Delta_H(P,h) = H(h) - H(h|P)$$

  (Notice $\Delta_H(P,h) \geq 0$)
- Easy to show that $\Delta_H(P,h) = 0$ iff the system leaks no information.
- hence $\Delta_H(P,h) = 0$ iff noninterference.
- But what does it mean when interference is positive?
- what does it mean $\Delta_H(P,h) = C > 0$
- what Δ_H (Cash machine,h)=0.00147 means?



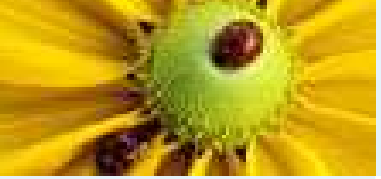
Quantitative analysis of confidentiality

difference of the measure F on the secret h before and after observing the system P

$$\Delta_H(P,h) = H(h) - H(h|P)$$

(Notice $\Delta_H(P,h) \geq 0$)

- Easy to show that $\Delta_H(P,h) = 0$ iff the system leaks no information.
- hence $\Delta_H(P,h) = 0$ iff noninterference.
- But what does it mean when interference is positive?
- what does it mean $\Delta_H(P,h) = C > 0$
- what Δ_H (Cash machine,h)=0.00147 means?
- for example why not 0.005?

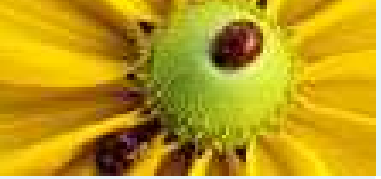


The Thermodynamics of Confidentiality

Consider again the leakage formula

$$\Delta_H(P, h) = H(h) - H(h|P)$$

- Define $W = H(h) - H(P)$, i.e. the difference between the initial and observations' uncertainty.

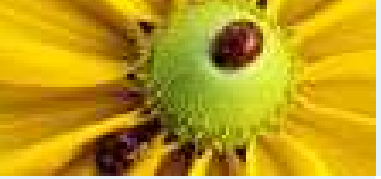


The Thermodynamics of Confidentiality

Consider again the leakage formula

$$\Delta_H(P, h) = H(h) - H(h|P)$$

- Define $W = H(h) - H(P)$, i.e. the difference between the initial and observations' uncertainty.
- Notice that (for deterministic systems) the following are equivalent to the above W

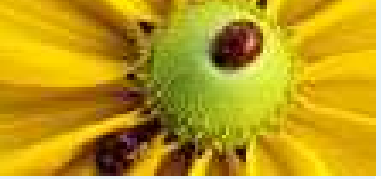


The Thermodynamics of Confidentiality

Consider again the leakage formula

$$\Delta_H(P, h) = H(h) - H(h|P)$$

- Define $W = H(h) - H(P)$, i.e. the difference between the initial and observations' uncertainty.
- Notice that (for deterministic systems) the following are equivalent to the above W
- $W = H(h|P)$ (=the remaining uncertainty)

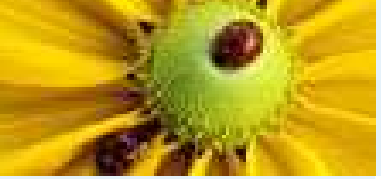


The Thermodynamics of Confidentiality

Consider again the leakage formula

$$\Delta_H(P,h) = H(h) - H(h|P)$$

- Define $W = H(h) - H(P)$, i.e. the difference between the initial and observations' uncertainty.
- Notice that (for deterministic systems) the following are equivalent to the above W
- $W = H(h|P)$ (=the remaining uncertainty)
- $W = H(h) - \Delta_H(P,h)$ (=what has not been leaked)

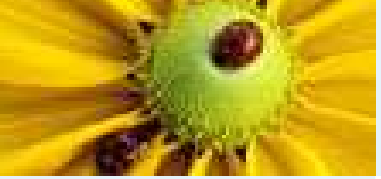


The Thermodynamics of Confidentiality

Consider again the leakage formula

$$\Delta_H(P,h) = H(h) - H(h|P)$$

- Define $W = H(h) - H(P)$, i.e. the difference between the initial and observations' uncertainty.
- Notice that (for deterministic systems) the following are equivalent to the above W
- $W = H(h|P)$ (=the remaining uncertainty)
- $W = H(h) - \Delta_H(P,h)$ (=what has not been leaked)
- we can see W as the cost to protect the secret...

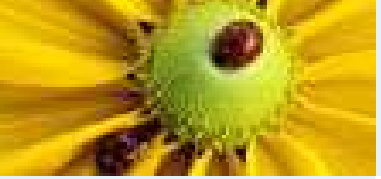


The Thermodynamics of Confidentiality

$$W = H(h) - H(P)$$

is the cost... cost of what?

- think of a computer in a room at temperature T.

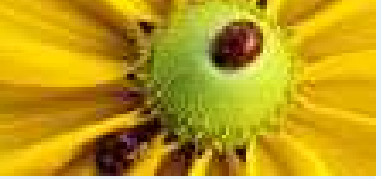


The Thermodynamics of Confidentiality

$$W = H(h) - H(P)$$

is the cost... cost of what?

- think of a computer in a room at temperature T.
- the computer has some energy cost to run

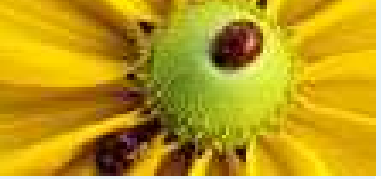


The Thermodynamics of Confidentiality

$$W = H(h) - H(P)$$

is the cost... cost of what?

- think of a computer in a room at temperature T.
- the computer has some energy cost to run
- this energy will be almost entirely transformed into heat

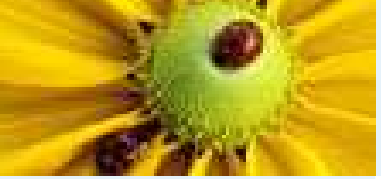


The Thermodynamics of Confidentiality

$$W = H(h) - H(P)$$

is the cost... cost of what?

- think of a computer in a room at temperature T.
- the computer has some energy cost to run
- this energy will be almost entirely transformed into heat
- W is the energy to be converted in heat to guarantee confidentiality.

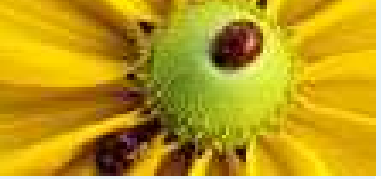


The Thermodynamics of Confidentiality

$$W = H(h) - H(P)$$

is the cost... cost of what?

- think of a computer in a room at temperature T.
- the computer has some energy cost to run
- this energy will be almost entirely transformed into heat
- W is the energy to be converted in heat to guarantee confidentiality.

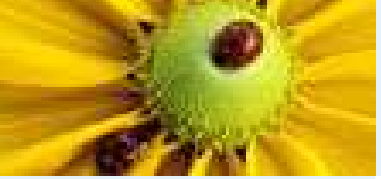


The Thermodynamics of Confidentiality

Given computation with leakage

$$\Delta_H(P, h) = H(h) - H(h|P)$$

- and P =final state of the system

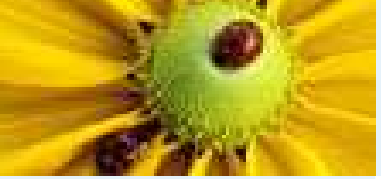


The Thermodynamics of Confidentiality

Given computation with leakage

$$\Delta_H(P, h) = H(h) - H(h|P)$$

- and P =final state of the system
- $W \ln(2) K_B T =$ minimum dissipation of any system implementing that computation ($K_B =$ Boltzmann constant, $T =$system temperature).

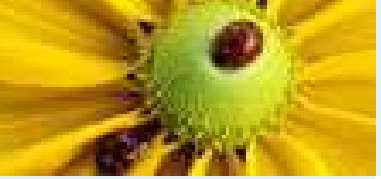


The Thermodynamics of Confidentiality

Given computation with leakage

$$\Delta_H(P,h) = H(h) - H(h|P)$$

- and P =final state of the system
- $W \ln(2) K_B T =$ minimum dissipation of any system implementing that computation ($K_B =$ Boltzmann constant, $T =$system temperature).
- ("The Thermodynamics of Confidentiality": Malacaria-Smeraldi CSF2012)



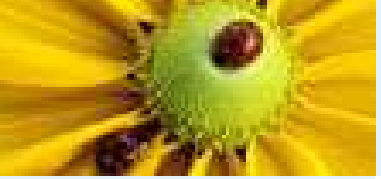
The Thermodynamics of Confidentiality

Given computation with leakage

$$\Delta_H(P,h) = H(h) - H(h|P)$$

- and P =final state of the system
- $W \ln(2) K_B T =$ minimum dissipation of any system implementing that computation ($K_B =$ Boltzmann constant, $T =$system temperature).
- ("The Thermodynamics of Confidentiality": Malacaria-Smeraldi CSF2012)
- e.g. security dissipation of a cash machine

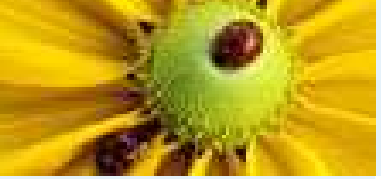
$$(13.2877124 - 0.00147) \ln(2) K_B T$$



The Thermodynamics of Confidentiality

$$13.28 \ln(2) K_B T$$

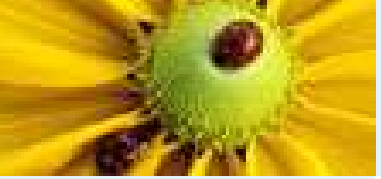
- very small... 8 orders of magnitude below current electronics, but...



The Thermodynamics of Confidentiality

$$13.28 \ln(2) K_B T$$

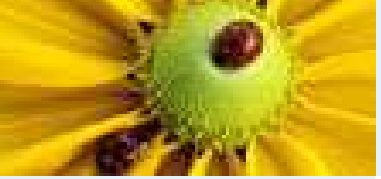
- very small... 8 orders of magnitude below current electronics, but...
- "Silicon-based technology is predicted to attain the Landauer limit ($\ln(2) K_B T$) in 20 to 30 years," (*Nature* (March 2012))



The Thermodynamics of Confidentiality

$$13.28 \ln(2) K_B T$$

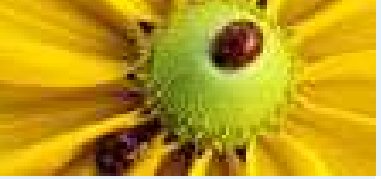
- very small... 8 orders of magnitude below current electronics, but...
- "Silicon-based technology is predicted to attain the Landauer limit ($\ln(2) K_B T$) in 20 to 30 years," (*Nature* (March 2012))
- there is a very active research in Physics on computing devices with“close to 0” dissipation :



The Thermodynamics of Confidentiality

$$13.28 \ln(2) K_B T$$

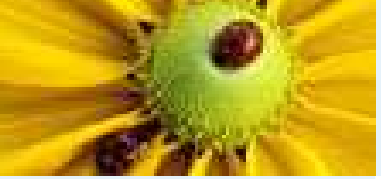
- very small... 8 orders of magnitude below current electronics, but...
- "Silicon-based technology is predicted to attain the Landauer limit ($\ln(2) K_B T$) in 20 to 30 years," (*Nature* (March 2012))
- there is a very active research in Physics on computing devices with“close to 0” dissipation :
- *Nature* (2011): implementation of Szilard engine, i.e. computation at near 0 dissipation.



The Thermodynamics of Confidentiality

$$13.28\ln(2)K_BT$$

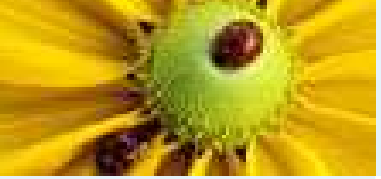
- very small... 8 orders of magnitude below current electronics, but...
- "Silicon-based technology is predicted to attain the Landauer limit ($\ln(2)K_BT$) in 20 to 30 years," (*Nature* (March 2012))
- there is a very active research in Physics on computing devices with“close to 0” dissipation :
- *Nature* (2011): implementation of Szilard engine, i.e. computation at near 0 dissipation.
- *Nature* (March 2012): “1 bit reset” cost at least $\ln(2)K_BT$.



The Thermodynamics of Confidentiality

$$13.28\,\ln(2)K_BT$$

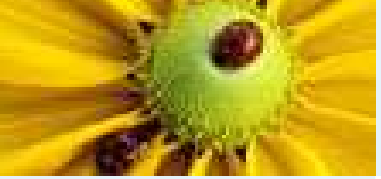
- very small... 8 orders of magnitude below current electronics, but...
- "Silicon-based technology is predicted to attain the Landauer limit ($\ln(2)K_BT$) in 20 to 30 years," (*Nature* (March 2012))
- there is a very active research in Physics on computing devices with“close to 0” dissipation :
- *Nature* (2011): implementation of Szilard engine, i.e. computation at near 0 dissipation.
- *Nature* (March 2012): “1 bit reset” cost at least $\ln(2)K_BT$.
- Confidentiality (W) is a lower bound on dissipation of computing devices



The Thermodynamics of Confidentiality

Confidentiality (W) is a lower bound on dissipation of computing devices

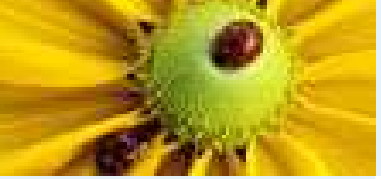
- a surprising consequence:



The Thermodynamics of Confidentiality

Confidentiality (W) is a lower bound on dissipation of computing devices

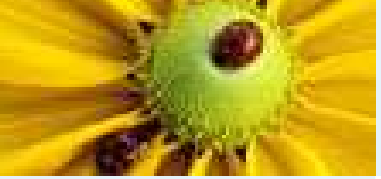
- a surprising consequence:
- a constant function “ do nothing”



The Thermodynamics of Confidentiality

Confidentiality (W) is a lower bound on dissipation of computing devices

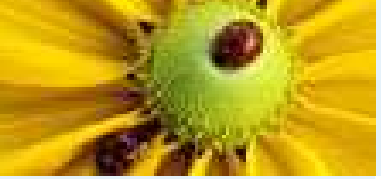
- a surprising consequence:
- a constant function “ do nothing”
- yet the computation of a constant function may heat more than any “difficult function”...



The Thermodynamics of Confidentiality

Confidentiality (W) is a lower bound on dissipation of computing devices

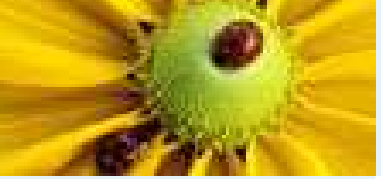
- a surprising consequence:
- a constant function “ do nothing”
- yet the computation of a constant function may heat more than any “difficult function”...
- (also calorimeters may detect leaks: if it should heat X and heats $Y << X$ instead then chances are there is an unwanted leak)



The Thermodynamics of Computation

Where is W coming from? It starts with Maxwell, and his demon...

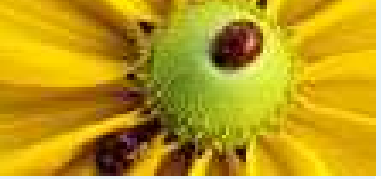
- Von Neumann: elementary (1 bit) computation dissipate $\ln(2)K_BT$



The Thermodynamics of Computation

Where is W coming from? It starts with Maxwell, and his demon...

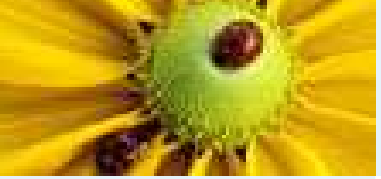
- Von Neumann: elementary (1 bit) computation dissipate $\ln(2)K_BT$
- Landauer: only elementary (1bit) irreversible computation dissipate $\ln(2)K_BT$



The Thermodynamics of Computation

Where is W coming from? It starts with Maxwell, and his demon...

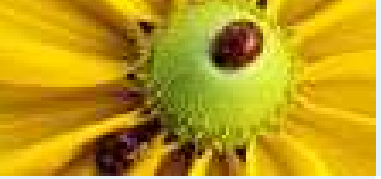
- Von Neumann: elementary (1 bit) computation dissipate $\ln(2)K_BT$
- Landauer: only elementary (1bit) irreversible computation dissipate $\ln(2)K_BT$
- Bennet: all computations can be made reversible, so no dissipation needed



The Thermodynamics of Computation

Where is W coming from? It starts with Maxwell, and his demon...

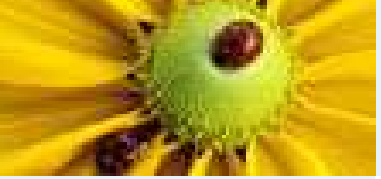
- Von Neumann: elementary (1 bit) computation dissipate $\ln(2)K_BT$
- Landauer: only elementary (1bit) irreversible computation dissipate $\ln(2)K_BT$
- Bennet: all computations can be made reversible, so no dissipation needed
- (good reference: Feynman Lectures in Computation)



The Thermodynamics of Computation

Where is W coming from? It starts with Maxwell, and his demon...

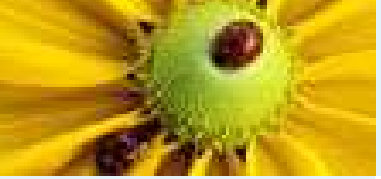
- Von Neumann: elementary (1 bit) computation dissipate $\ln(2)K_BT$
- Landauer: only elementary (1bit) irreversible computation dissipate $\ln(2)K_BT$
- Bennet: all computations can be made reversible, so no dissipation needed
- (good reference: Feynman Lectures in Computation)
- confidentiality needs irreversibility



The Thermodynamics of Computation

Where is W coming from? It starts with Maxwell, and his demon...

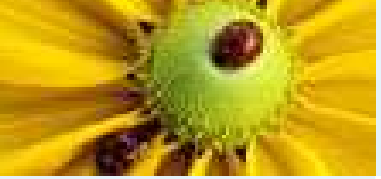
- Von Neumann: elementary (1 bit) computation dissipate $\ln(2)K_BT$
- Landauer: only elementary (1bit) irreversible computation dissipate $\ln(2)K_BT$
- Bennet: all computations can be made reversible, so no dissipation needed
- (good reference: Feynman Lectures in Computation)
- confidentiality needs irreversibility
- how much irreversibility?



The Thermodynamics of Computation

Where is W coming from? It starts with Maxwell, and his demon...

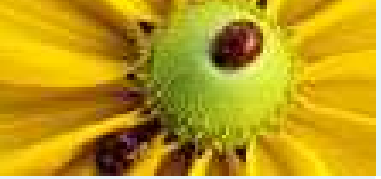
- Von Neumann: elementary (1 bit) computation dissipate $\ln(2)K_BT$
- Landauer: only elementary (1bit) irreversible computation dissipate $\ln(2)K_BT$
- Bennet: all computations can be made reversible, so no dissipation needed
- (good reference: Feynman Lectures in Computation)
- confidentiality needs irreversibility
- how much irreversibility?
- exactly W



The Thermodynamics of Computation

Where is W coming from? It starts with Maxwell, and his demon...

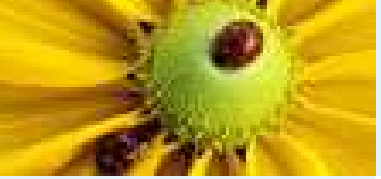
- Von Neumann: elementary (1 bit) computation dissipate $\ln(2)K_BT$
- Landauer: only elementary (1bit) irreversible computation dissipate $\ln(2)K_BT$
- Bennet: all computations can be made reversible, so no dissipation needed
- (good reference: Feynman Lectures in Computation)
- confidentiality needs irreversibility
- how much irreversibility?
- exactly W
- This is what 0.00147 mean...



The Thermodynamics of Confidentiality

Notice we assumed the system to be deterministic... What if the system is probabilistic?

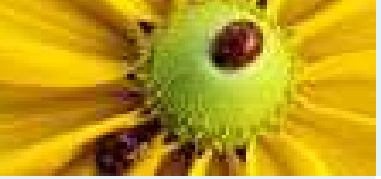
- a register containing a secret may be randomised instead of being reset



The Thermodynamics of Confidentiality

Notice we assumed the system to be deterministic... What if the system is probabilistic?

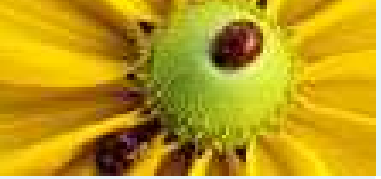
- a register containing a secret may be randomised instead of being reset
- (here we are thinking of truly random processes, not `Math.random()`...)



The Thermodynamics of Confidentiality

Notice we assumed the system to be deterministic... What if the system is probabilistic?

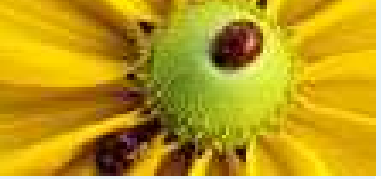
- a register containing a secret may be randomised instead of being reset
- (here we are thinking of truly random processes, not `Math.random()`...)
- what happen then?



The Thermodynamics of Confidentiality

Notice we assumed the system to be deterministic... What if the system is probabilistic?

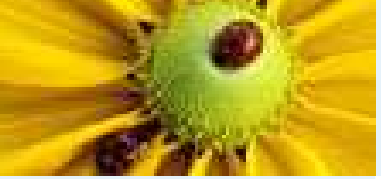
- That's why we defined $W = H(h) - H(P)$ and not $W = H(h|P)$



The Thermodynamics of Confidentiality

Notice we assumed the system to be deterministic... What if the system is probabilistic?

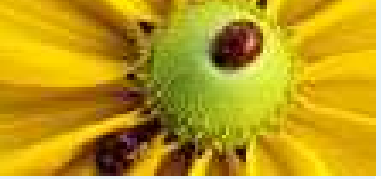
- That's why we defined $W = H(h) - H(P)$ and not $W = H(h|P)$
- for probabilistic systems W can be negative:



The Thermodynamics of Confidentiality

Notice we assumed the system to be deterministic... What if the system is probabilistic?

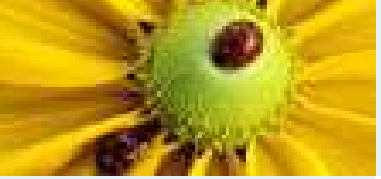
- That's why we defined $W = H(h) - H(P)$ and not $W = H(h|P)$
- for probabilistic systems W can be negative:
- the randomization process inject entropy in the system,



The Thermodynamics of Confidentiality

Notice we assumed the system to be deterministic... What if the system is probabilistic?

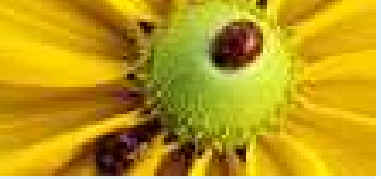
- That's why we defined $W = H(h) - H(P)$ and not $W = H(h|P)$
- for probabilistic systems W can be negative:
- the randomization process inject entropy in the system,
- that means that "work" can be extracted by the system...



The Thermodynamics of Confidentiality

Notice we assumed the system to be deterministic... What if the system is probabilistic?

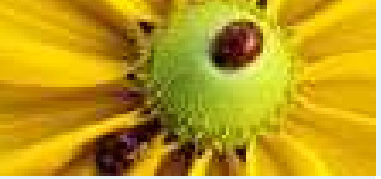
- That's why we defined $W = H(h) - H(P)$ and not $W = H(h|P)$
- for probabilistic systems W can be negative:
- the randomization process inject entropy in the system,
- that means that "work" can be extracted by the system...
- when W is negative $W \ln(2) K_B T$ is the work that can be extracted by the system.



The Thermodynamics of Confidentiality

Notice we assumed the system to be deterministic... What if the system is probabilistic?

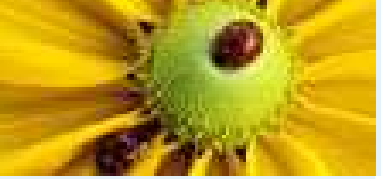
- That's why we defined $W = H(h) - H(P)$ and not $W = H(h|P)$
- for probabilistic systems W can be negative:
- the randomization process inject entropy in the system,
- that means that "work" can be extracted by the system...
- when W is negative $W \ln(2) K_B T$ is the work that can be extracted by the system.
- It is not a free lunch: it needs to be paid back to return the system to its initial state...



A clarification about power analysis:

Very successful crypto attacks are based on heat dissipation (power analysis attacks on smart cards): deduce what path in the circuit was taken by a computation by measuring power consumption.

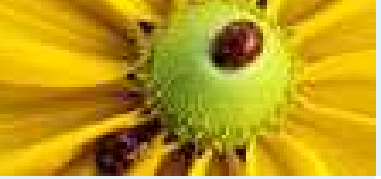
- From that path infer (part of) the secret.



A clarification about power analysis:

Very successful crypto attacks are based on heat dissipation (power analysis attacks on smart cards): deduce what path in the circuit was taken by a computation by measuring power consumption.

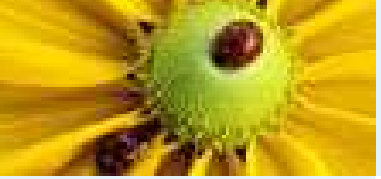
- From that path infer (part of) the secret.
- These attacks are due to technology inefficiencies, not to fundamental physical laws.



A clarification about power analysis:

Very successful crypto attacks are based on heat dissipation (power analysis attacks on smart cards): deduce what path in the circuit was taken by a computation by measuring power consumption.

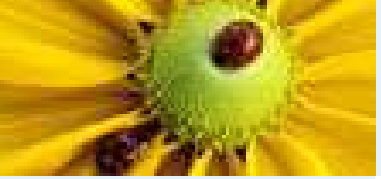
- From that path infer (part of) the secret.
- These attacks are due to technology inefficiencies, not to fundamental physical laws.
- Cryptography is (mathematically trivially) reversible so efficient technology will moderated these attacks.



A clarification about power analysis:

Very successful crypto attacks are based on heat dissipation (power analysis attacks on smart cards): deduce what path in the circuit was taken by a computation by measuring power consumption.

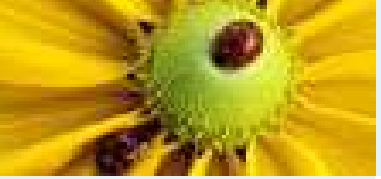
- From that path infer (part of) the secret.
- These attacks are due to technology inefficiencies, not to fundamental physical laws.
- Cryptography is (mathematically trivially) reversible so efficient technology will moderated these attacks.
- But W cannot be moderated...



Alternative measures of knowledge:

$$\Delta_F(P,h) = F(h) - F(h|P)$$

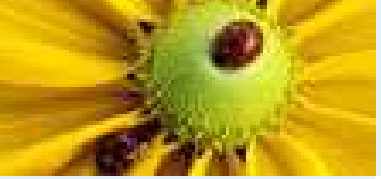
- What about choosing a different F? is there still a physical meaning?



Alternative measures of knowledge:

$$\Delta_F(P,h) = F(h) - F(h|P)$$

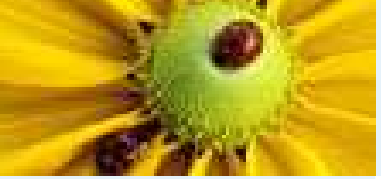
- What about choosing a different F? is there still a physical meaning?
- *Probability of guessing in one try:* (introduced by Smith and noted ME)



Alternative measures of knowledge:

$$\Delta_F(P,h) = F(h) - F(h|P)$$

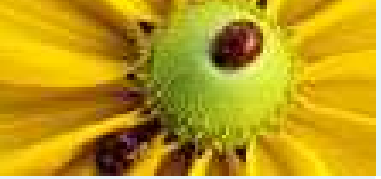
- What about choosing a different F? is there still a physical meaning?
- *Probability of guessing in one try:* (introduced by Smith and noted ME)
- $F(h) = G(h) = -\log(\max_{x \in h} \mu(h = x)) =$ a priory probability of guessing h



Alternative measures of knowledge:

$$\Delta_F(P,h) = F(h) - F(h|P)$$

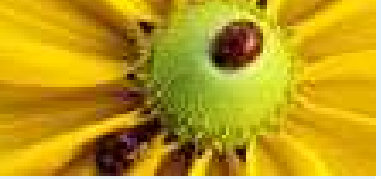
- What about choosing a different F? is there still a physical meaning?
- *Probability of guessing in one try:* (introduced by Smith and noted ME)
- $F(h) = G(h) = -\log(\max_{x \in h} \mu(h = x)) =$ a priory probability of guessing h
- $F(h|P) = G(h|P) = -\log(\sum_{y \in P} \mu(y)(\max_{x \in h} \mu(h = x|P = y))) =$ probability of guessing h given observations



Alternative measures of knowledge:

$$\Delta_F(P,h) = F(h) - F(h|P)$$

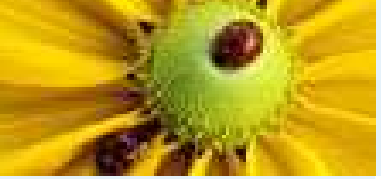
- What about choosing a different F? is there still a physical meaning?
- *Probability of guessing in one try:* (introduced by Smith and noted ME)
- $F(h) = G(h) = -\log(\max_{x \in h} \mu(h = x)) =$ a priory probability of guessing h
- $F(h|P) = G(h|P) = -\log(\sum_{y \in P} \mu(y)(\max_{x \in h} \mu(h = x|P = y))) =$ probability of guessing h given observations
- Δ_{ME} (Cash machine,h)=1 ($= \log(2)$): chances have doubled)



The Thermodynamics of guessability

$$\Delta_{ME}(P,h) = G(h) - G(h|P)$$

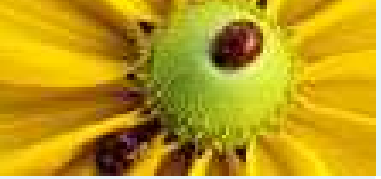
- $G(h|P) \leq W$



The Thermodynamics of guessability

$$\Delta_{ME}(P,h) = G(h) - G(h|P)$$

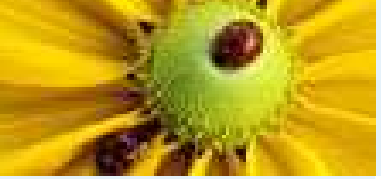
- $G(h|P) \leq W$
- $G(h|P) = W$ iff the system initial and final states are maximally disordered (e.g. a program computing $h\%m$)



The Thermodynamics of guessability

$$\Delta_{ME}(P,h) = G(h) - G(h|P)$$

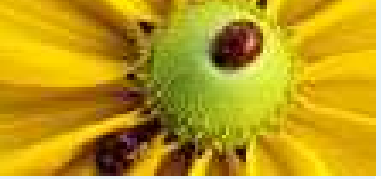
- $G(h|P) \leq W$
- $G(h|P) = W$ iff the system initial and final states are maximally disordered (e.g. a program computing $h\%m$)
- Intruiging: first “connection” between guessabiity and thermodynamics...



Conclusions

Measures of interference have a profound physical meaning.

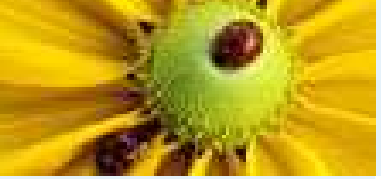
- They relate to fundamental limits of computing devices



Conclusions

Measures of interference have a profound physical meaning.

- They relate to fundamental limits of computing devices
- and to cutting edge research in Physics;



Conclusions

Measures of interference have a profound physical meaning.

- They relate to fundamental limits of computing devices
- and to cutting edge research in Physics;
- they give a fresh angle on the thermodynamics of computation.