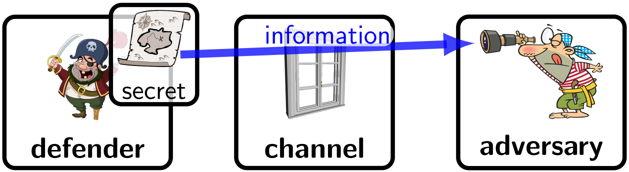
Quantifying Information Flow for Dynamic Secrets

Piotr (Peter) Mardziel,[†] Mário S. Alvim,[+] Michael Hicks,[†] and Michael R. Clarkson[*]

[†]University of Maryland, College Park,
[+]Universidade Federal de Minas Gerais,
[*]George Washington University and Cornell University

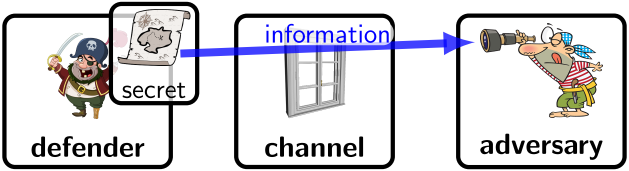
Quantified Information Flow [QIF]

- Secrets leak to bad guys.
- **Quantify leakage of the secret.**



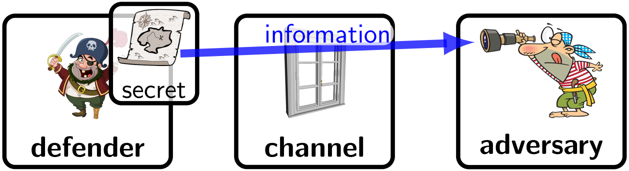
Why Quantified Information Flow?

- Evaluate risks.
- Evaluate relative merits of protection mechanisms.
- Design incentives to keep adversaries from participating.



Examples

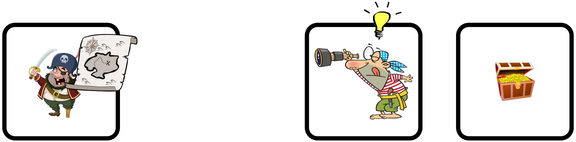
- Password authentication
- Location-based services
- Address space randomization



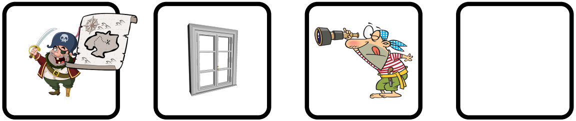
Quantified Information Flow: The Approach

- **Flow** $\stackrel{\text{def}}{=}$ increase in adversary's expected success
  - Model channel.
  - Model adversary behavior, exploitation.
  - Quantify expected success of optimal adversary.

before observation

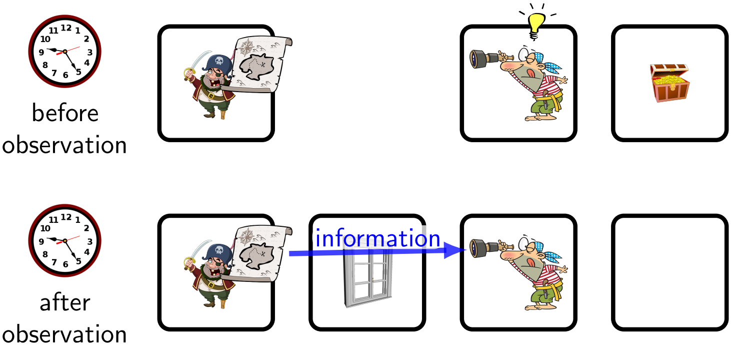


after observation



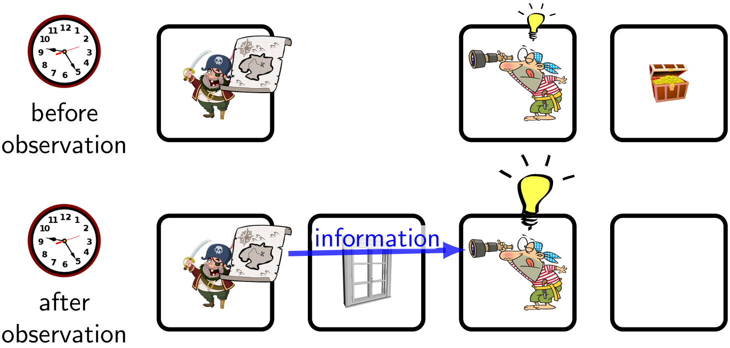
Quantified Information Flow: The Approach

- **Flow** $\stackrel{\text{def}}{=}$ increase in adversary's expected success
  - Model channel.
  - Model adversary behavior, exploitation.
  - Quantify expected success of optimal adversary.



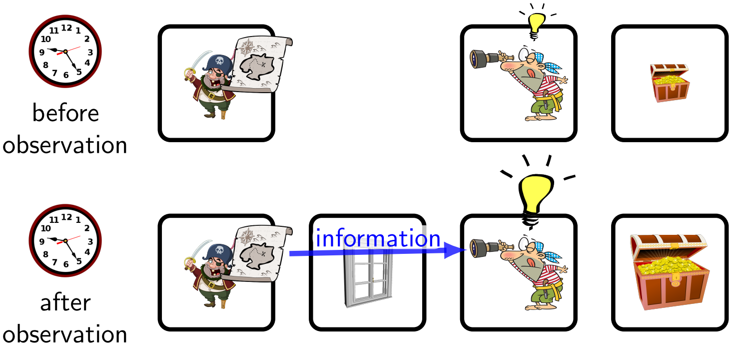
Quantified Information Flow: The Approach

- **Flow** $\stackrel{\text{def}}{=}$ increase in adversary's expected success
  - Model channel.
  - Model adversary behavior, exploitation.
  - Quantify expected success of optimal adversary.



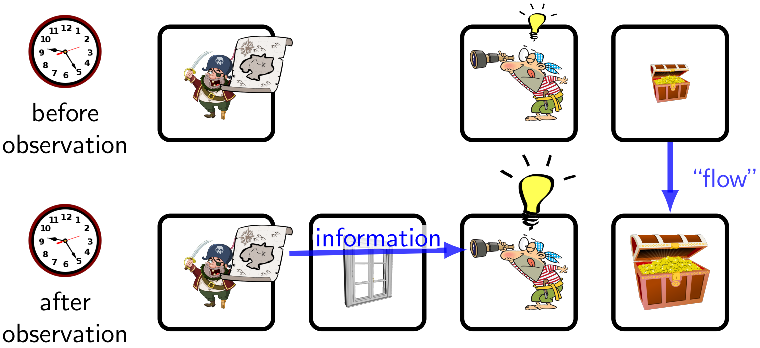
Quantified Information Flow: The Approach

- **Flow** $\stackrel{\text{def}}{=}$ increase in adversary's expected success
  - Model channel.
  - Model adversary behavior, exploitation.
  - Quantify expected success of optimal adversary.



Quantified Information Flow: The Approach

- **Flow** $\stackrel{\text{def}}{=}$ increase in adversary's expected success
  - Model channel.
  - Model adversary behavior, exploitation.
  - Quantify expected success of optimal adversary.



This work: define flow when the secret can change

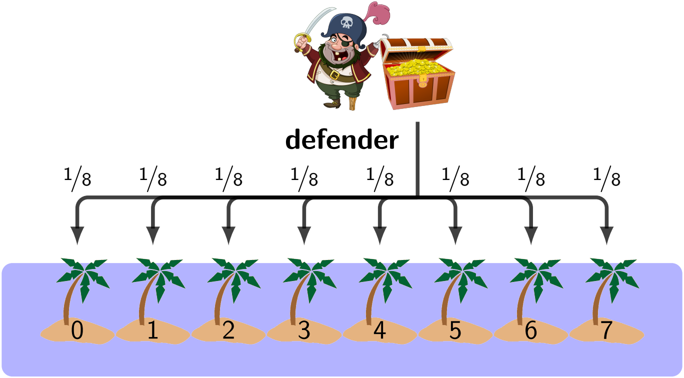
- Defined formal model for scenarios with dynamic secrets.
  - Accommodates adaptive adversaries.
  - More expressive than prior models.
- Definition of flow generalizes prior measures.
- Demonstrated several interesting phenomena using an implementation of our model.
  - Low-adaptive adversary $\Rightarrow$ exponentially higher flow.
  - Wait-adaptive adversary $\Rightarrow$ monotonically increasing flow.
  - More change does not necessarily mean more security.

Outline

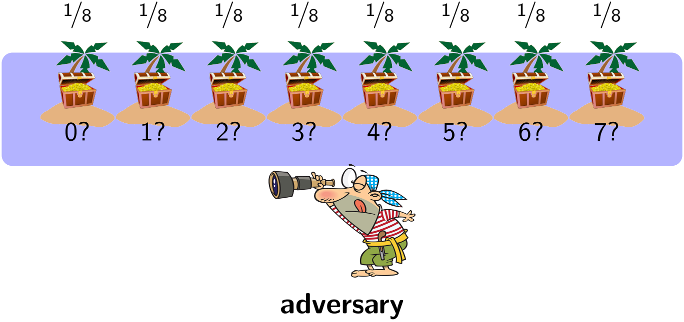
- Example: Static secrets
  - Low-adaptive adversaries decide how to influence the channel based on prior observations.
  - Low-adaptivity $\Rightarrow$ exponentially higher flow.
- Example: Dynamic secrets
  - Wait-adaptive adversaries decide when to exploit the secret.
  - Wait adaptivity $\Rightarrow$ monotonically increasing flow with time.

Example: Pirate Treasure



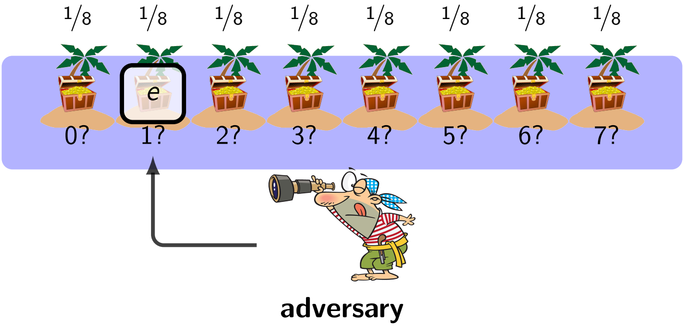
Secret Prior

Secret Prior = Defender Belief



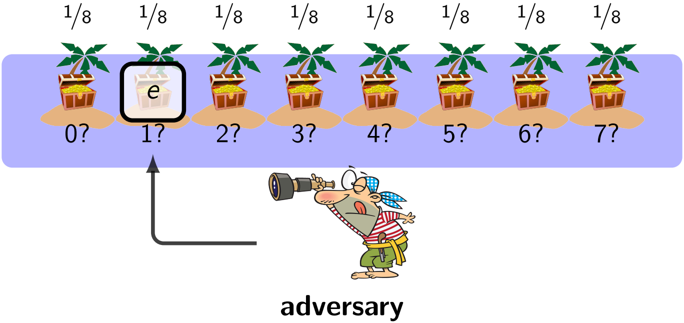
- Assumption: adversary knows defender behavior.

Exploitation



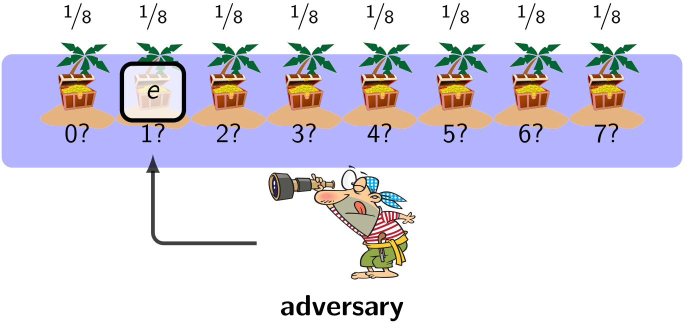
- Adversary "raids" an island e for the treasure. If $e = h$ he succeeds.

Exploitation



- Smith (FoSSaCS '09): (prior) **Vulnerability**: expected probability of optimal adversary with one guess being correct.

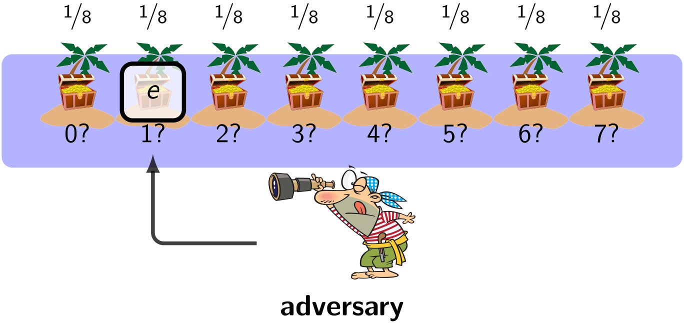
Exploitation: Measures of Success



Optimal adversary behavior:

- **Guessing Entropy**: Minimal number of guesses to find secret.
- Alvim et al. (CSF '12): g-**Vulnerability** Gain/payoff according to function $g(\mathrm{secret}, \mathrm{exploit})$.

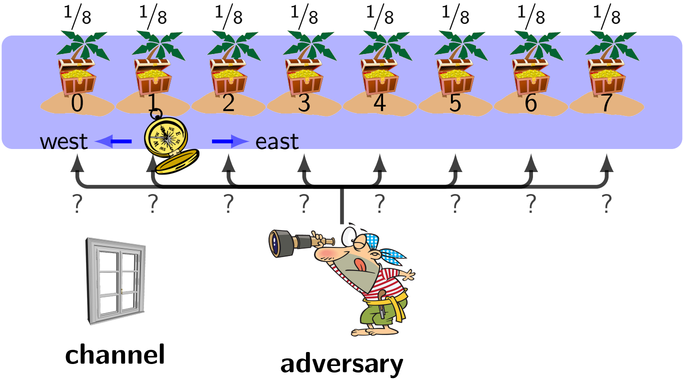
Exploitation: Vulnerability



- Connect probability of success to economic quantities.
- If the treasure is worth w doubloons, the expected gain to adversary and loss to the defender is $w \times \mathbb{V}$ doubloons. Here, $^{w}\!/_{8}$.
- Will stick with expected probability of success using the term "gain" in the remainder of this talk.

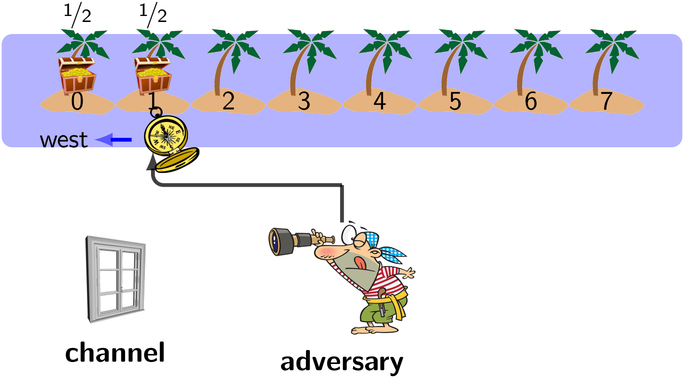
Observation

- Gold compass points in the direction of the treasure.
- Adversary has a choice of where to use the compass.
- Analogy to timing side-channel in an RSA implementation as per Brumley and Boneh (USENIX Security '03)



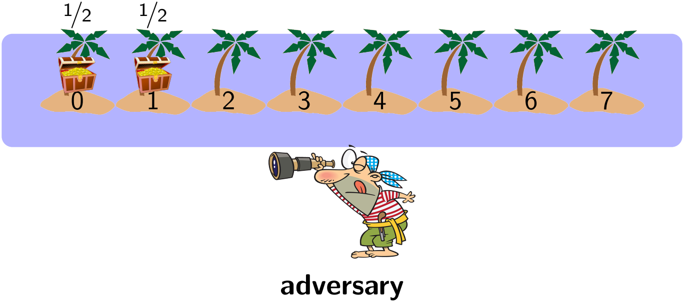
Observation

- Gold compass points in the direction of the treasure.
- Adversary has a choice of where to use the compass.
- Analogy to timing side-channel in an RSA implementation as per Brumley and Boneh (USENIX Security '03)



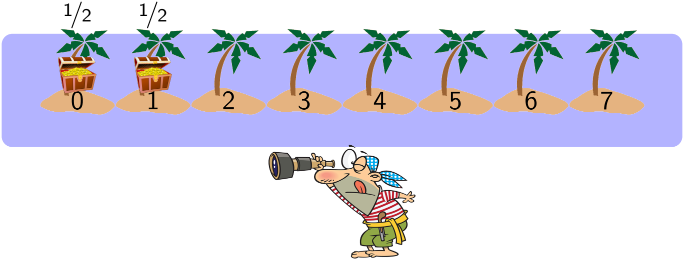
Increased knowledge

- Observation leads to increase in knowledge.
- Which leads to increased odds of exploitation.



Increased knowledge ⇒ increased gain

- (posterior) **Gain**: expected probability of optimal adversary succeeding in one guess **given observation(s)**.



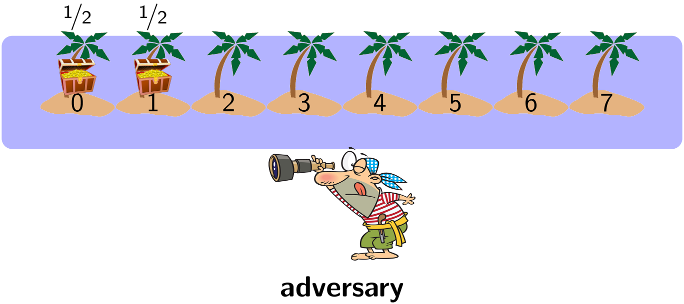
adversary

Increased knowledge ⇒ increased gain

- (posterior) **Gain**: expected probability of optimal adversary succeeding in one guess **given observation(s)**.
- Optimize adversary strategy:

  $\alpha : \{\text{east}, \text{west}\} \rightarrow \{0, \cdots, 7\}$.

  - island to raid given the observation

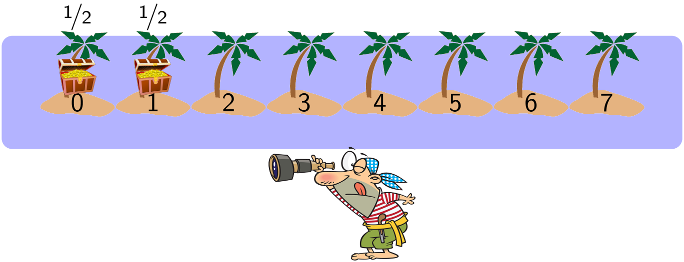


Increased knowledge ⇒ increased gain

- (posterior) **Gain**: expected probability of optimal adversary succeeding in one guess **given observation(s)**.
- Optimize adversary strategy:

  $\alpha : \{\text{east}, \text{west}\} \rightarrow \boxed{\{0, \cdots, 7\}}$.

  - island to raid given the observation



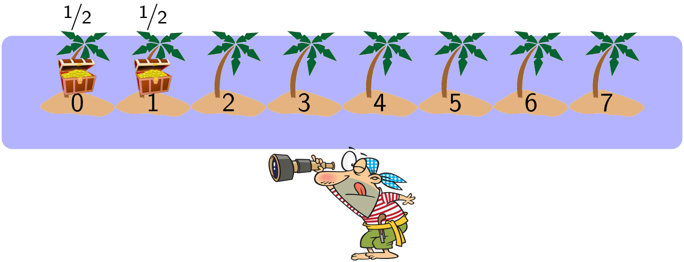
adversary

Increased knowledge ⇒ increased gain

- (posterior) **Gain**: expected probability of optimal adversary succeeding in one guess **given observation(s)**.
- Optimize adversary strategy:

  $\alpha : \{\text{east}, \text{west}\} \rightarrow \{0, \cdots, 7\}$.

  - island to raid given the observation



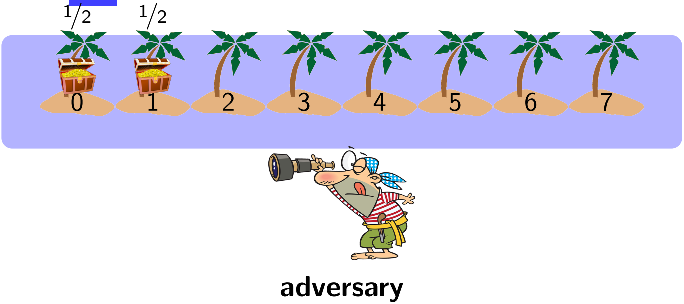
adversary

Increased knowledge $\Rightarrow$ increased gain

- (posterior) **Gain**: expected probability of optimal adversary succeeding in one guess **given observation(s)**.
- Optimize adversary strategy:

  $\alpha : \{\text{east}, \text{west}\} \rightarrow \{0, \cdots, 7\}$.

  - island to raid given the observation
- Here: $\boxed{2/8}$.



Observations over time

- Assume locations of compass use are fixed ahead of time: $\ell_1, \ell_2, \cdots$.
- (max) time $= 1$: observe at ℓ_1, optimize $\{\text{east}, \text{west}\} \to \{0, \cdots, 7\}$
  Island to raid given compass observation at island ℓ_1.

Observations over time

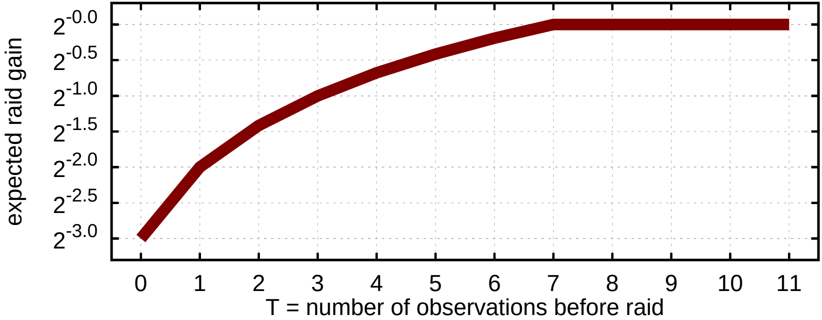
- Assume locations of compass use are fixed ahead of time: $\ell_1, \ell_2, \cdots$.
- (max) time $= 1$: observe at ℓ_1, optimize $\{\text{east}, \text{west}\} \to \{0, \cdots, 7\}$
- (max) time $= 2$: observe at ℓ_2, optimize $\alpha : \{\text{east}, \text{west}\} \times \{\text{east}, \text{west}\} \to \{0, \cdots, 7\}$.
  Island to raid given compass observations at islands ℓ_1 and ℓ_2.

Observations over time

- Assume locations of compass use are fixed ahead of time: $\ell_1, \ell_2, \cdots$.
- (max) time = 1: observe at ℓ_1, optimize $\{\text{east}, \text{west}\} \to \{0, \cdots, 7\}$
- (max) time = 2: observe at ℓ_2, optimize $\alpha : \{\text{east}, \text{west}\} \times \{\text{east}, \text{west}\} \to \{0, \cdots, 7\}$.
- (max) time = T ...

Observations over time

- Assume locations of compass use are fixed ahead of time: $\ell_1, \ell_2, \cdots$.
- (max) time $= 1$: observe at ℓ_1, optimize $\{\text{east}, \text{west}\} \to \{0, \cdots, 7\}$
- (max) time $= 2$: observe at ℓ_2, optimize $\alpha : \{\text{east}, \text{west}\} \times \{\text{east}, \text{west}\} \to \{0, \cdots, 7\}$.
- (max) time $= T$ ...



Where to observe?

- Low adaptivity: adversary uses prior observations to choose how to observe next.

Where to observe?

- Low adaptivity: adversary uses prior observations to choose how to observe next.
  - Optimize how to observe:

    $$\alpha_\ell : \{0_\ell, \cdots, 7_\ell\}^{t-1} \times \{\text{east}, \text{west}\}^{t-1} \to \{0_\ell, \cdots, 7_\ell\} .$$

Where to observe?

- Low adaptivity: adversary uses prior observations to choose how to observe next.
  - Optimize how to observe:

    $\alpha_\ell : \{0_\ell, \cdots, 7_\ell\}^{t-1} \times \{\mathrm{east}, \mathrm{west}\}^{t-1} \to \boxed{\{0_\ell, \cdots, 7_\ell\}}$.

Where to observe?

- Low adaptivity: adversary uses prior observations to choose how to observe next.
  - Optimize how to observe:

    $\alpha_\ell : \{0_\ell, \cdots, 7_\ell\}^{t-1} \times \boxed{\{\text{east}, \text{west}\}^{t-1}} \to \{0_\ell, \cdots, 7_\ell\}$.

Where to observe?

- Low adaptivity: adversary uses prior observations to choose how to observe next.
  - Optimize how to observe:
    $\alpha_\ell : \boxed{\{0_\ell, \cdots, 7_\ell\}^{t-1}} \times \{\text{east}, \text{west}\}^{t-1} \rightarrow \{0_\ell, \cdots, 7_\ell\}$.

Where to observe?

- Low adaptivity: adversary uses prior observations to choose how to observe next.
  - Optimize how to observe:

    $\alpha_\ell : \{0_\ell, \cdots, 7_\ell\}^{t-1} \times \{\text{east}, \text{west}\}^{t-1} \rightarrow \{0_\ell, \cdots, 7_\ell\}$.
  - Optimize how to exploit:

    $\alpha_e : \{0_\ell, \cdots, 7_\ell\}^{t} \times \{\text{east}, \text{west}\}^{t} \rightarrow \{0_e, \cdots, 7_e\}$.

Where to observe?

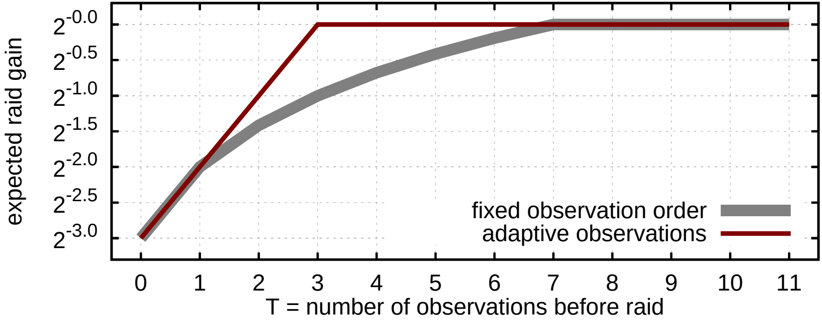
- Low adaptivity: adversary uses prior observations to choose how to observe next.
  - Optimize how to observe:

    $\alpha_\ell : \{0_\ell, \cdots, 7_\ell\}^{t-1} \times \{\text{east}, \text{west}\}^{t-1} \to \{0_\ell, \cdots, 7_\ell\}$.
  - Optimize how to exploit:

    $\alpha_e : \boxed{\{0_\ell, \cdots, 7_\ell\}^{t} \times \{\text{east}, \text{west}\}^{t}} \to \{0_e, \cdots, 7_e\}$.

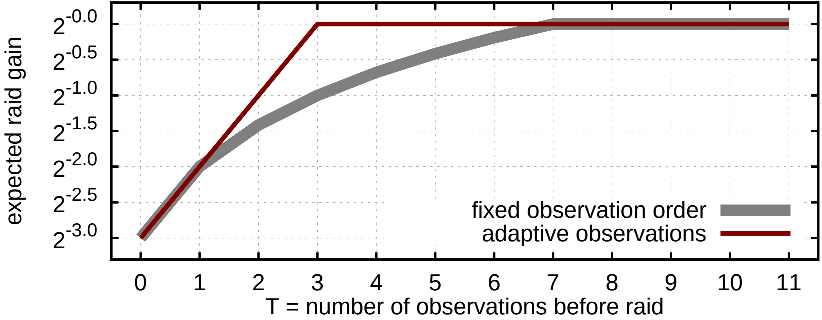
Where to observe?

- Low adaptivity: adversary uses prior observations to choose how to observe next.
  - Optimize how to observe:
    $\alpha_\ell : \{0_\ell, \cdots, 7_\ell\}^{t-1} \times \{\text{east}, \text{west}\}^{t-1} \to \{0_\ell, \cdots, 7_\ell\}$.
  - Optimize how to exploit:
    $\alpha_e : \{0_\ell, \cdots, 7_\ell\}^{t} \times \{\text{east}, \text{west}\}^{t} \to \{0_e, \cdots, 7_e\}$.
  - Can perform binary search for the secret (cannot do so with fixed observation order)

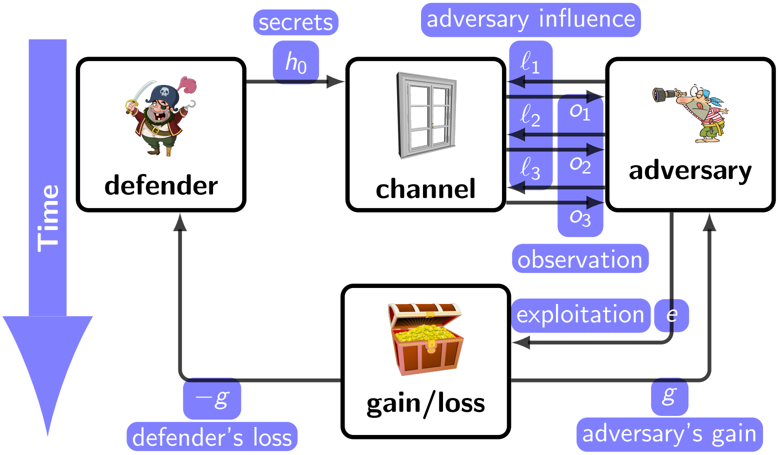


Low Adaptivity

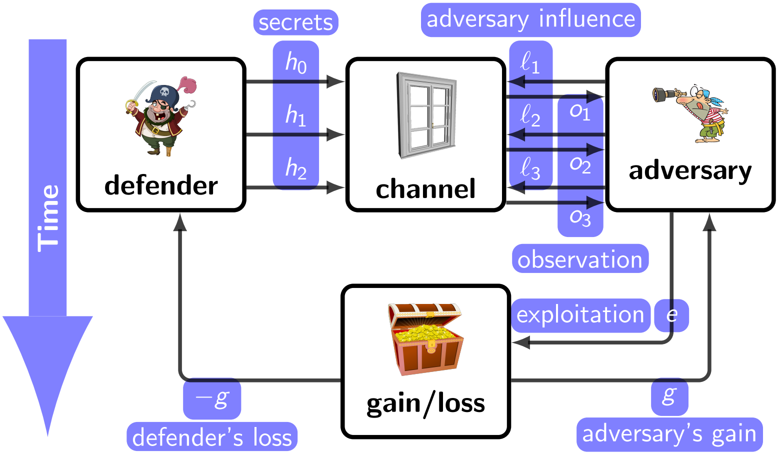
- Köpf and Basin (CCS '07): low-adaptive adversaries for deterministic systems (side channels).
- Adaptivity is largely ignored in QIF literature (even since the above work).
- **Our work: probabilistic systems (channel, defender behavior).**



Overview so far

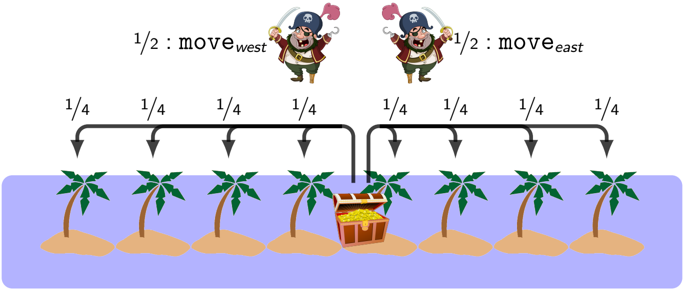


Add dynamic secrets



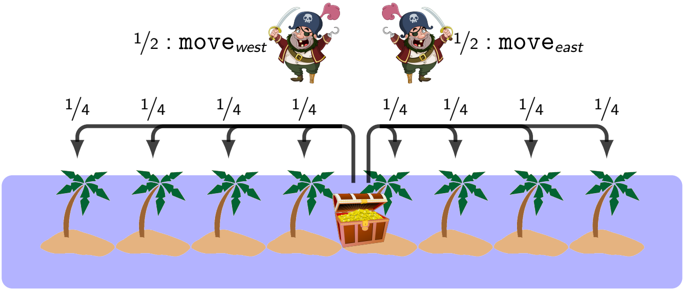
Example: Moving treasure

- Defender's strategy changes the secret based on prior secret.
- Prior, he chooses one of two strategies with equal probability.



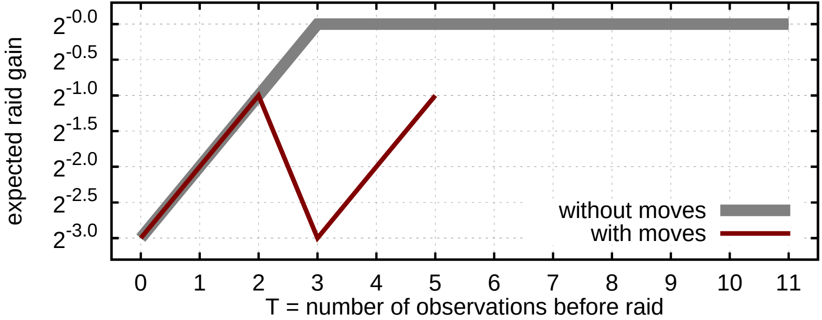
Example: Moving treasure

- Defender's strategy changes the secret based on prior secret.
- Prior, he chooses one of two strategies with equal probability.
- **Assumption**: adversary knows the process with which the defender chose his strategy (but not the resulting strategy).



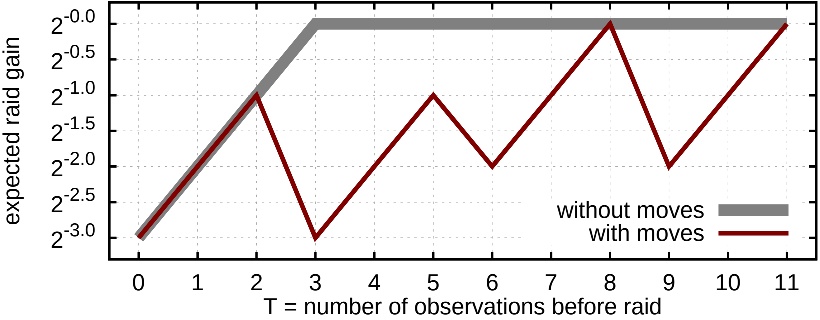
Gain with moving treasure

- Defender moves his treasure every 3 time steps.



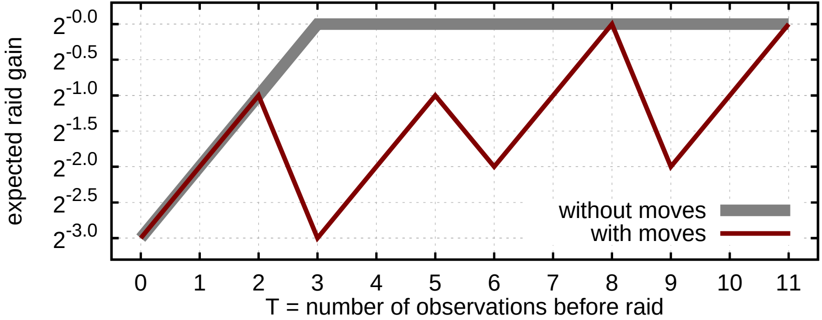
Gain with moving treasure

- Defender moves his treasure every 3 time steps.



Gain with moving treasure

- Defender moves his treasure every 3 time steps.
- Adversary eventually learns how the treasure moves.

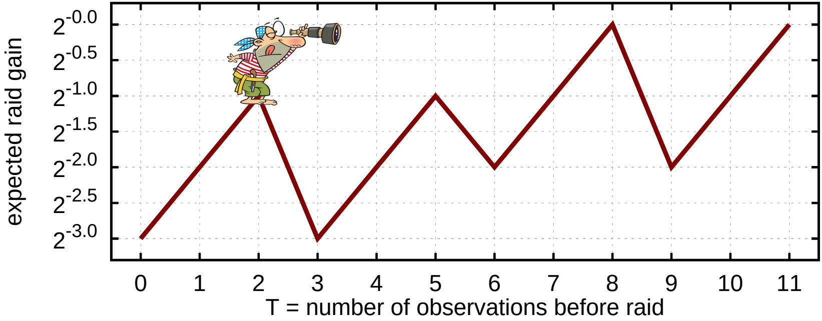


Hiding the treasure vs. Hiding its dynamics

- Uneasy balance:
  - Protect secrecy of current secret.
  - Protect secrecy of how the secret changes.
- This can lead to strangeness: more secret change $\Rightarrow$ quicker adversary inference of secret (see paper).

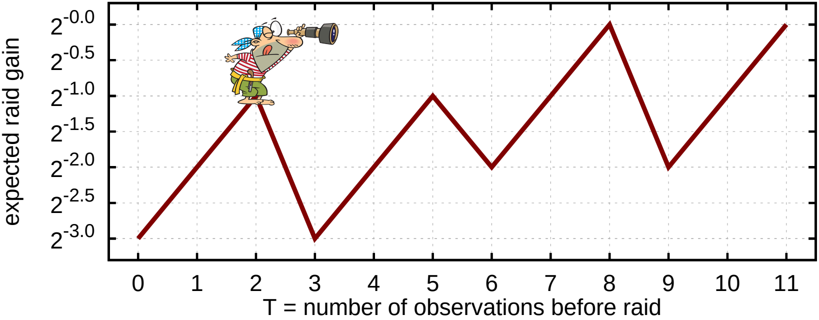
Negative flow?

- Gain at time 3 < Gain at time 2



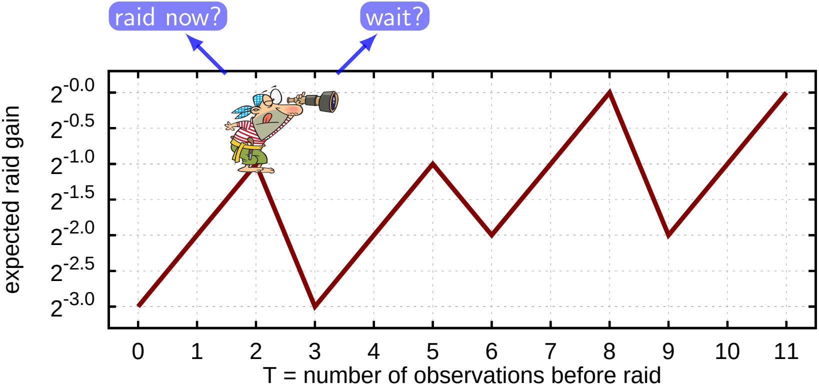
Negative flow?

- Gain at time 3 $<$ Gain at time 2
- Problem: Gain at time T: adversary makes exactly T observations then raids.



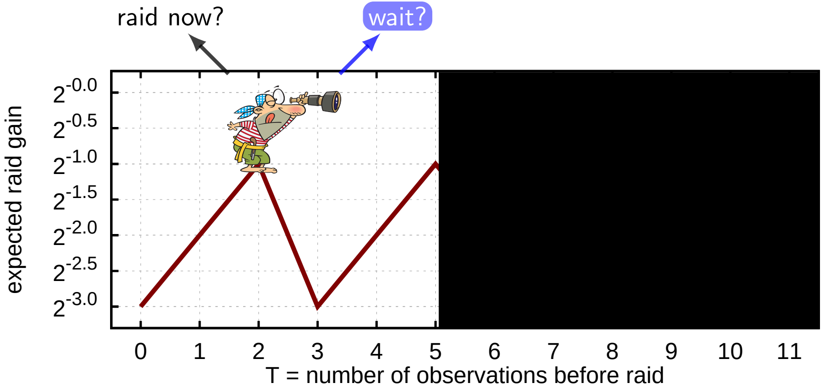
Negative flow?

- Gain at time 3 $<$ Gain at time 2
- Problem: Gain at time T: adversary makes exactly T observations then raids.
- Solution: Gain at time T: adversary makes at most T observations then raids.



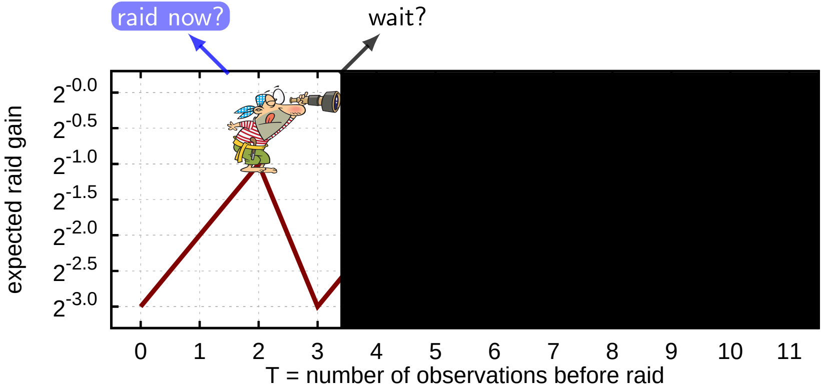
Negative flow?

- Gain at time 3 < Gain at time 2
- Problem: Gain at time T: adversary makes exactly T observations then raids.
- Solution: Gain at time T: adversary makes at most T observations then raids.



Negative flow?

- Gain at time 3 < Gain at time 2
- Problem: Gain at time T: adversary makes exactly T observations then raids.
- Solution: Gain at time T: adversary makes at most T observations then raids.



Adaptive wait

- Adaptive-wait adversary: decides when to exploit based on prior observations.
  $\alpha : \{0_\ell, \cdots, 7_\ell\}^t \times \{\text{east}, \text{west}\}^t \rightarrow \{0_\ell, \cdots, 7_\ell\} \cup \{0_e, \cdots, 7_e\}$

Adaptive wait

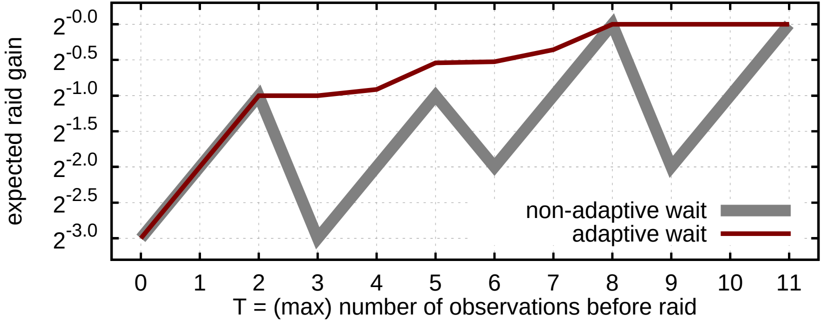
- Adaptive-wait adversary: decides when to exploit based on prior observations.
  $\alpha : \{0_\ell, \cdots, 7_\ell\}^t \times \{\text{east}, \text{west}\}^t \to \{0_\ell, \cdots, 7_\ell\} \cup \{0_e, \cdots, 7_e\}$

Adaptive wait

- Adaptive-wait adversary: decides when to exploit based on prior observations.
  $\alpha : \{0_\ell, \cdots, 7_\ell\}^t \times \{\text{east}, \text{west}\}^t \rightarrow \{0_\ell, \cdots, 7_\ell\} \cup \{0_e, \cdots, 7_e\}$

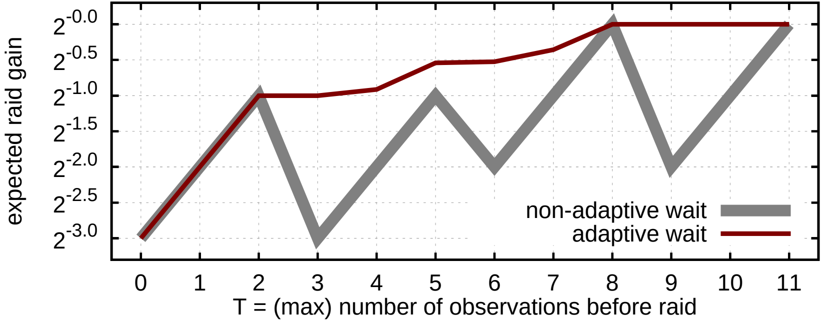
Adaptive wait

- Adaptive-wait adversary: decides when to exploit based on prior observations.
  $\alpha : \{0_\ell, \cdots, 7_\ell\}^t \times \{\mathrm{east}, \mathrm{west}\}^t \to \{0_\ell, \cdots, 7_\ell\} \cup \{0_e, \cdots, 7_e\}$
- Monotonic gain over time (positive flow).



Adaptive wait

- Adaptive-wait adversary: decides when to exploit based on prior observations.
  $\alpha : \{0_\ell, \cdots, 7_\ell\}^t \times \{\mathrm{east}, \mathrm{west}\}^t \rightarrow \{0_\ell, \cdots, 7_\ell\} \cup \{0_e, \cdots, 7_e\}$
- Monotonic gain over time (positive flow).
- "Non-compositional": optimal behavior for time 3 is not the prefix to optimal behavior for time 5.



Prototype Implementation

- Describe models as probabilistic programs in monadic-style OCaml.
- Optimize adversary behavior via backward induction.
- Analyze a series of scenarios (including this talk's examples)
- Freely available online.

Conclusions



- Model for information flow with dynamic secrets.

Conclusions

- Model for information flow with dynamic secrets.
- Handling of adaptive adversary behavior.

Conclusions

- Model for information flow with dynamic secrets.
- Handling of adaptive adversary behavior.
  - <u>Low adaptivity</u> $\Rightarrow$ exponential increase in gain.
  - <u>Wait adaptivity</u> $\Rightarrow$ monotonically increasing gain.

Conclusions

- Model for information flow with dynamic secrets.
- Handling of adaptive adversary behavior.
  - Low adaptivity $\Rightarrow$ exponential increase in gain.
  - Wait adaptivity $\Rightarrow$ monotonically increasing gain.
- Most expressive model for QIF to date (as far as we know)

Conclusions



- Model for information flow with dynamic secrets.
- Handling of adaptive adversary behavior.
  - Low adaptivity $\Rightarrow$ exponential increase in gain.
  - Wait adaptivity $\Rightarrow$ monotonically increasing gain.
- Most expressive model for QIF to date (as far as we know)
- Implementation and Experiments
  - More change $\Rightarrow$ more gain
  - And more! (see paper and TR)

Quantifying Information Flow for Dynamic Secrets

http://ter.ps/dqif

- Model for information flow with dynamic secrets.
- Handling of adaptive adversary behavior.
  - Low adaptivity $\Rightarrow$ exponential increase in gain.
  - Wait adaptivity $\Rightarrow$ monotonically increasing gain.
- Most expressive model for QIF to date (as far as we know)
- Implementation and Experiments
  - More change $\Rightarrow$ more gain
  - And more! (see paper and TR)
- `http://ter.ps/dqif`
  - Paper, TR, Implementation, Experiments
  - Follow up paper: adversary gain $\neq$ defender loss