Does It Really Help to Run Challenge-Response Protocols Repeatedly ?

Max Kanovich, Tajana Ban Kirigin, Vivek Nigam,
Andre Scedrov, and Carolyn Talcott.

The aim of this work

1. **A general method** to provide **the full probabilistic analysis** of **the Attack in Between Ticks** (and its **variations**) on Distance-Bounding Protocols, established by Kanovich, Kirigin, Nigam, Scedrov, and Talcott [POST 2015]

2. We **challenge a general belief** that Verifier can improve their performance by means of collecting statistics *in a long series of n challenge-response rounds*.

   Can we **mitigate** or **even rule out** the attacks on Distance-Bounding Protocols by using challenge-response rounds repeatedly ?

   "Yes" and **"No"**

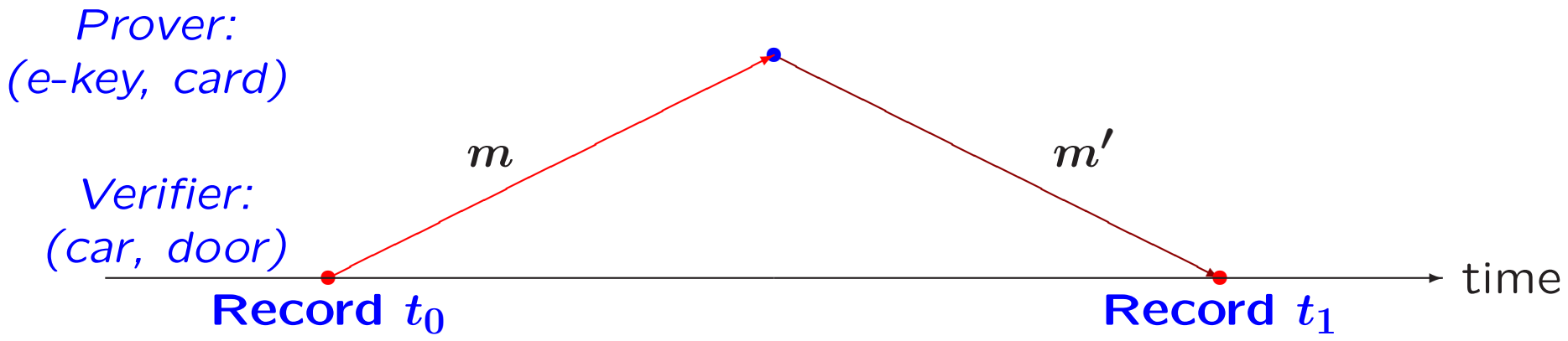
Cyber-Physical Security Protocols

Cyber-Physical Security Protocols are security protocols which **rely upon the physical properties** in which their protocol sessions are carried out, such as:

- message transmission takes time;
- processing requests takes time;
- different transmission channels and velocities;
- *physical and network distances between participants*.

Distance Bounding Protocols

The round trip time of messages and **the transmission velocity** are taken into account to **infer an upper bound on the distance** between two agents, **to identify them correctly**.



If the **measured** $t_1 - t_0 \leq R$ for a given *time response bound*, R, then the Verifier grants the access to its resources to the Prover.

The Challenge-Response Protocol (in terms of the atomic actions)

- Assume $\boldsymbol{R} = 4$;

- Verifier needs to perform four atomic operations:

(1) Send Challenge;

(2) Record the fact that the message was sent;

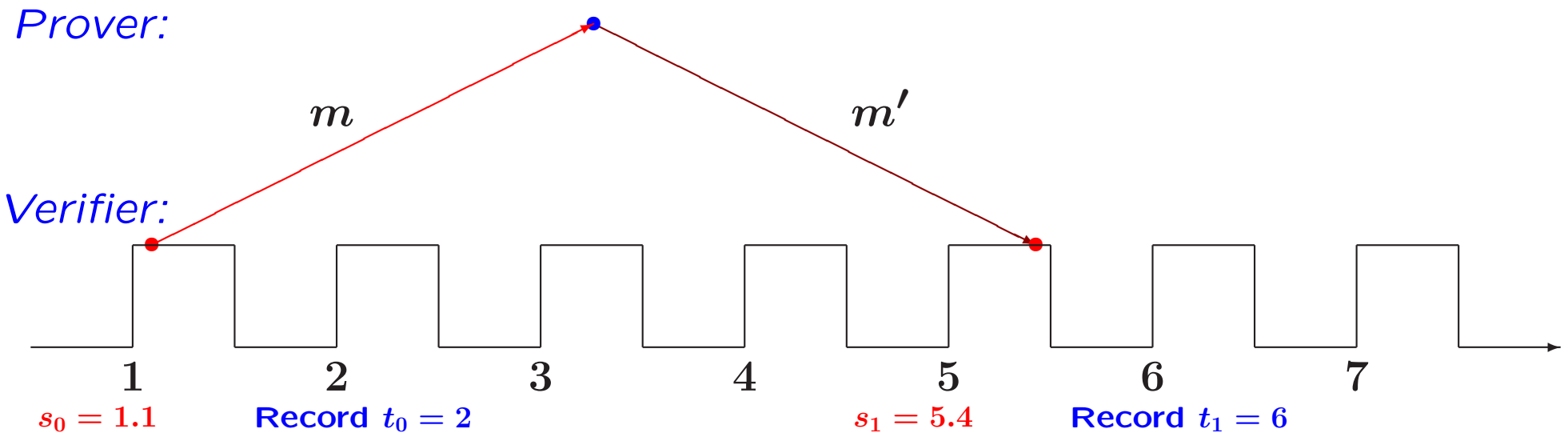
(3) Receive Response;

(4) Record the fact that the response has been received.

Abstract Verifier against Actual Verifier

- **Abstract Verifier**
  - Operates in **dense time**;
  - **An unbounded number of timed events** are allowed within *any small time interval*. Zeno's Paradox.
- **Actual Verifier**
  - Operates in **discrete time** at a finite clock rate;
  - Only **a fixed finite number** of events may occur within a bounded time interval.
  - W.l.o.g., we assume here that the Actual Verifier can execute **no more than one operation in one clock cycle**.
  - E.g., the *sending or receiving* of a signal must occur in **a different clock cycle** than the *measurement* of the current time.

Attack in Between Ticks (Actual Verifier, $R = 4$)



- Verifier has got to **grant access**, since for **the measured** $t_1 - t_0$,

$$t_1 - t_0 = 4 \leq R$$

- Though, **the actual round trip time is greater than** R **!**

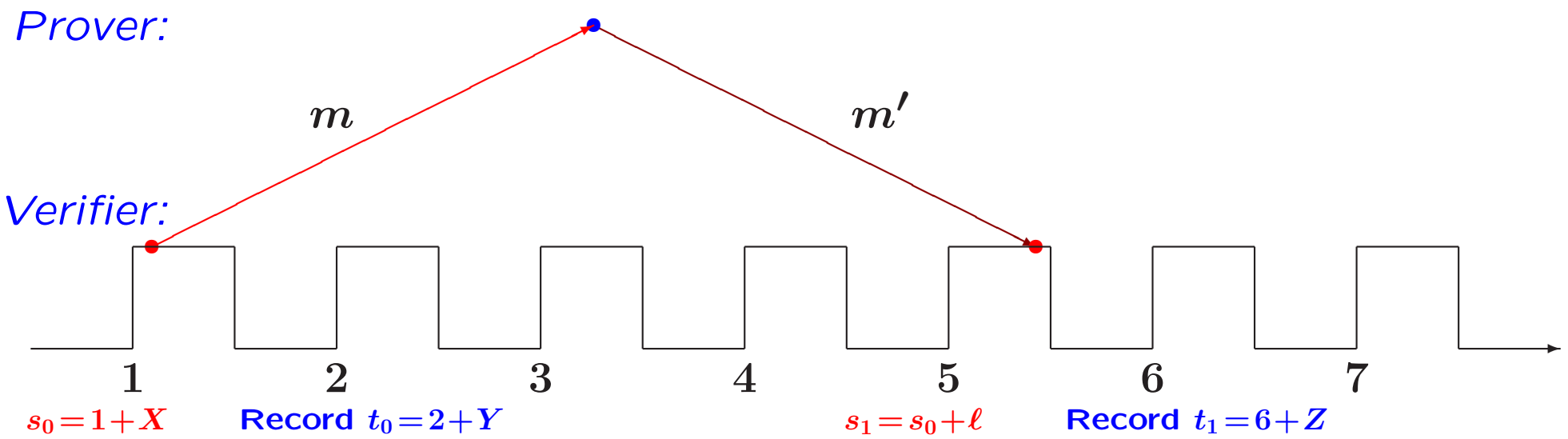
$$\ell = s_1 - s_0 = 4.3 > R$$

What has it got to do with reality ?

The difference between **the actual round trip time** and the measured trip time can be of **one clock tick** even if each operation is executed in one clock cycle.

- **1 clock cycle of a 24MHz processor = 42 ns;**
- Light travels 30cm in 1ns;
- Thus the error can be of **12.6 meters round trip**.
  The mismatch can be used by the attacker to pretend that he is **6.3 meters closer to Verifier than he actually is**.

The challenge-response protocol (Actual Verifier)



$$\begin{cases} s_0 = 1 + X, & s_1 = s_0 + \ell, \\ t_0 = 2 + Y, & t_1 = \lfloor s_1 \rfloor + 1 + Z. \end{cases}$$

X, Y, and Z are random variables distributed on $[0, \frac{1}{2}]$.

When the decision is erroneous "$t_1 - t_0$" against "$s_1 - s_0$"

In the talk we are dealing with the system:

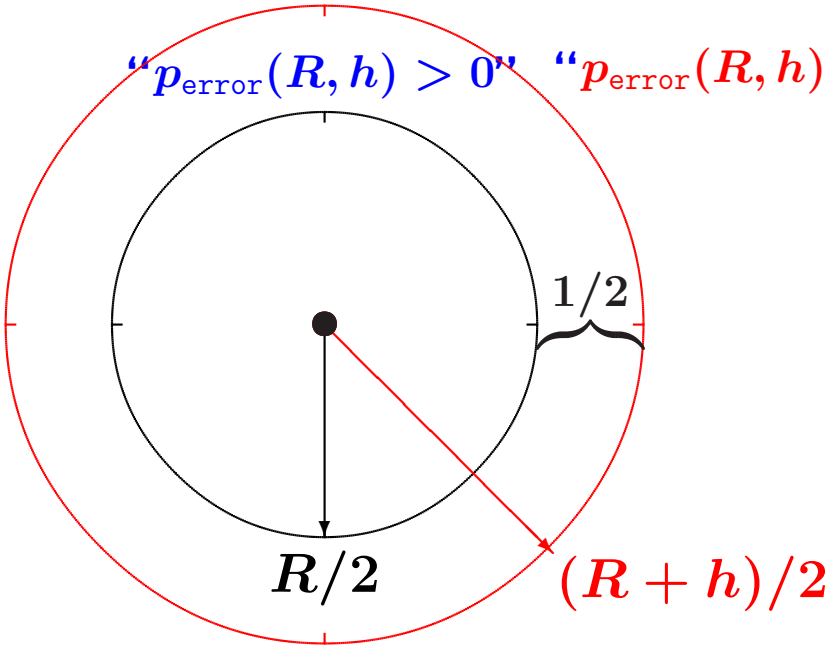
$$\begin{cases} s_0 = 1 + X, & s_1 = s_0 + \ell, \\ t_0 = 2 + Y, & t_1 = \lfloor s_1 \rfloor + 1 + Z. \end{cases}$$

The "Yes" decision (caused by the *measured* $t_1 - t_0 \le R$) is taken as **erroneous**, if in reality the *actual distance*, $s_1 - s_0$, turns out to be larger than R, say by some positive *excess/extra*, h.

$p_{\mathrm{error}}(R, h)$, *the probability of the erroneous decision*, is defined as the conditional probability:

$$\mathrm{p_{error}(R, h)} = \mathtt{Prob}\,\{\, \mathrm{t_1 - t_0 \le R} \mid \mathrm{s_1 - s_0 = R + h} \,\} \qquad (1)$$

The probability of the erroneous decision (Thm 12.1, R is an integer)



$$p_{\text{error}}(R,h) = \begin{cases} \frac{1}{2}, & \text{if } 0 < h \le \frac{1}{2}, \\ 1-h, & \text{if } \frac{1}{2} < h < 1, \\ 0, & \text{if } h \ge 1. \end{cases}$$

The probability of the erroneous decision

Theorem 12.1 *Let Y and Z be distributed with one and the same density, an arbitrary g.*
Let X be uniformly distributed on $[0, \frac{1}{2}]$.
Then, for a fixed time response bound, an integer R, and an extra, a positive h,

$$p_{\mathtt{error}}(R,h) = \begin{cases} \frac{1}{2}, & \text{if } 0 < h \leq \frac{1}{2}, \\ 1-h, & \text{if } \frac{1}{2} < h < 1, \\ 0, & \text{if } h \geq 1. \end{cases} \qquad (2)$$

The probability of the erroneous decision

Theorem 12.1 *Let Y and Z be distributed with one and the same density,* an arbitrary g.
Let X be uniformly distributed on $[0, \frac{1}{2}]$.
Then, for a fixed time response bound, an integer R, *and an extra,* a positive h,

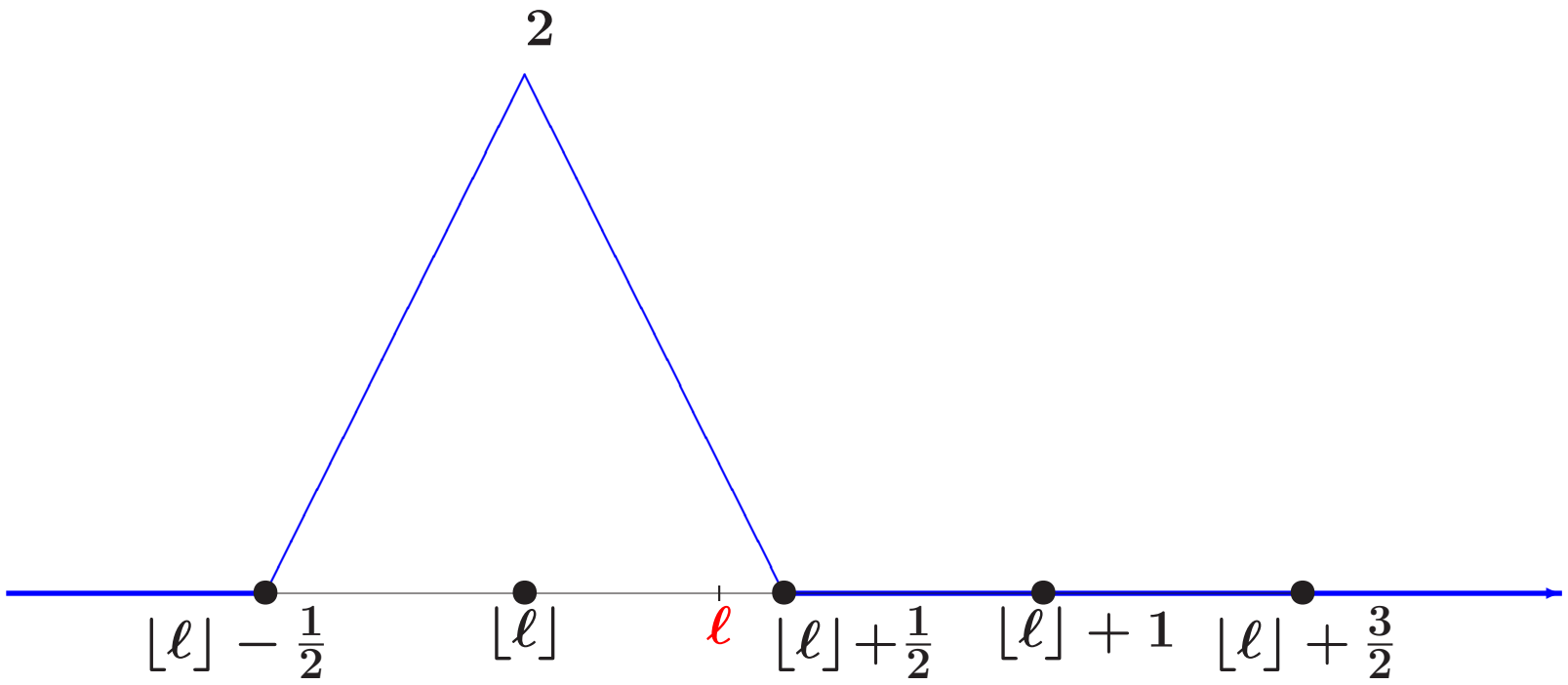
$$p_{\mathtt{error}}(R,h) = \begin{cases} \frac{1}{2}, & \text{if } 0 < h \leq \frac{1}{2}, \\ 1-h, & \text{if } \frac{1}{2} < h < 1, \\ 0, & \text{if } h \geq 1. \end{cases} \qquad (2)$$

Comment 12.1 The formula in Thm 12.1 is *one and the same*, *whatever peculiar distribution density g for Y and Z we take !*

("Dromedary camel" case) $\widetilde{\ell} = \ell - \lfloor \ell \rfloor \le \frac{1}{2}$.

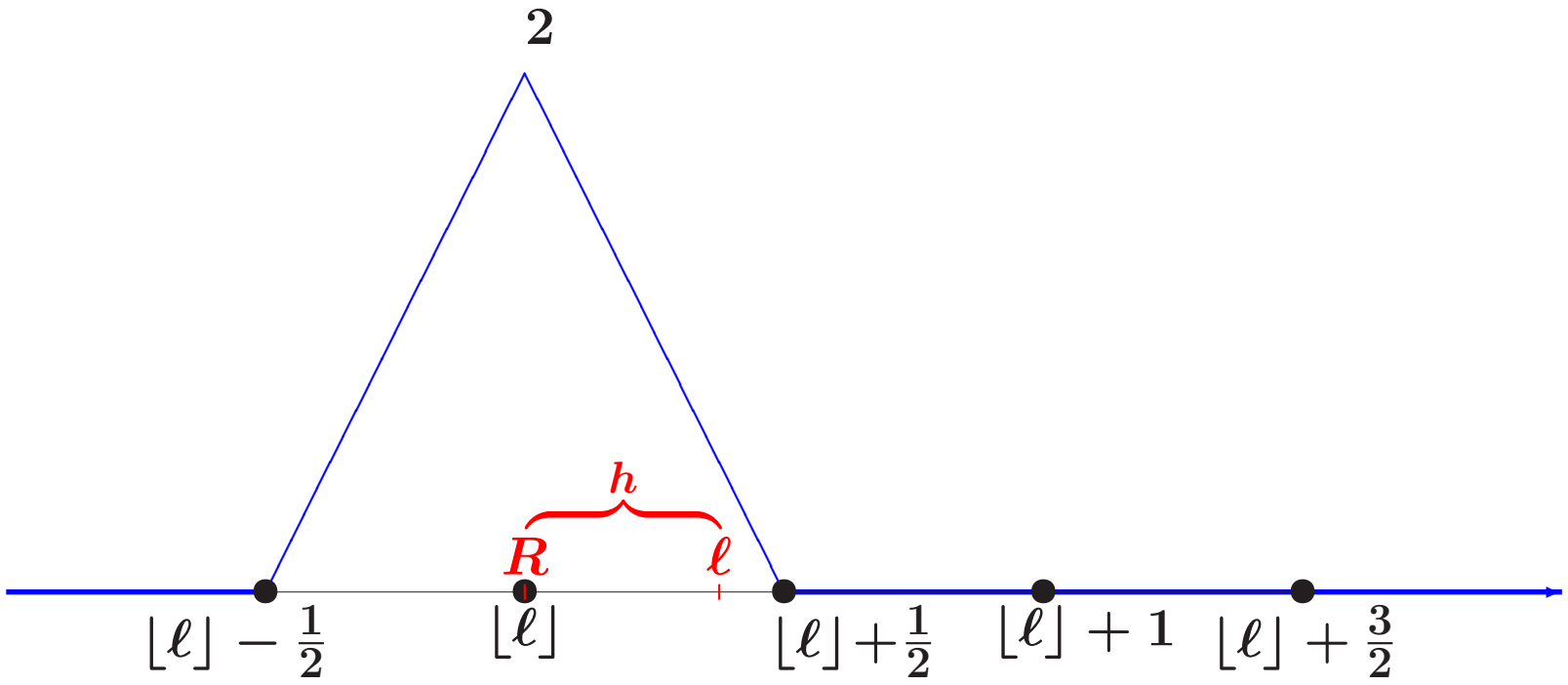
The graph of the density, $F'_\ell(w)$, for the distribution $F_\ell(w)$:

$$F_\ell(w) = \texttt{Prob}\{\ t_1 - t_0 \le w \mid s_1 - s_0 = \ell\ \}$$



$F'_\ell(w)$ is always 'symmetrical' whenever $f_Y = f_Z$.

Thm 12.1, Proof: $p_{\texttt{error}}(R,h) = \frac{1}{2}$, if $0 < h \leq \frac{1}{2}$

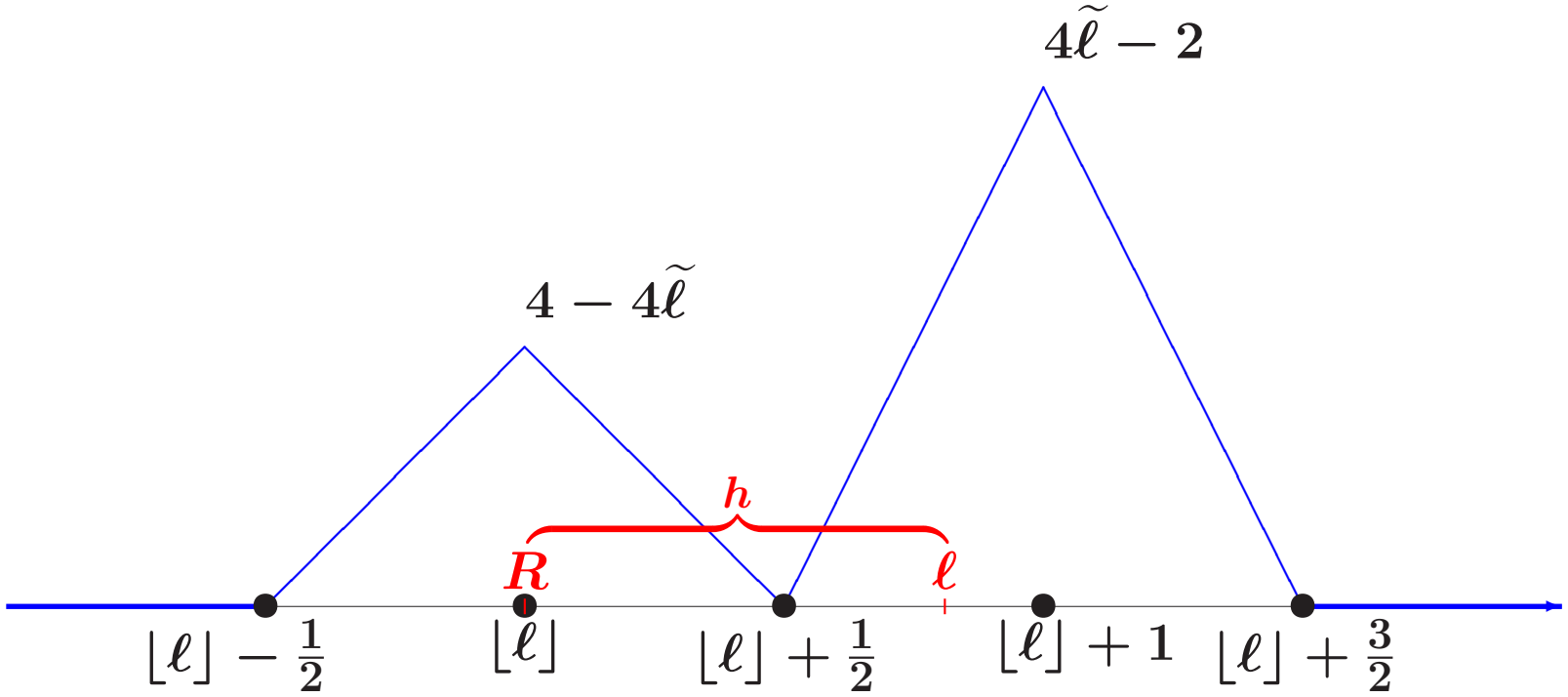


Given an integer R, let $\ell = R + h$. Then $\lfloor \ell \rfloor = R$, and

$$p_{\texttt{error}}(R,h) = \int_{-\infty}^{\lfloor \ell \rfloor} F'_{\ell}(w)\, dw = \frac{1}{2}$$

Thm 12.1 ("Bactrian camel" case: two humps)

Proof: $p_{\mathtt{error}}(R,h) = 1-h$, if $\frac{1}{2} < h < 1$



Given an integer R, let $\ell = R + h$. Then $\lfloor \ell \rfloor = R$, and

$$p_{\mathtt{error}}(R,h) = \int_{-\infty}^{\lfloor \ell \rfloor} F'_{\ell}(w)\, dw = 1 - \widetilde{\ell} = 1 - h$$

Using challenge-response rounds repeatedly ?

- We **challenge a general belief** that Verifier can improve their performance by means of collecting statistics *in a long series of n challenge-response rounds*.

- How can we **formalize** this "improve their performance"

- Can we **mitigate** or **even rule out** the attacks on Distance-Bounding Protocols by using challenge-response rounds repeatedly ?

  "Yes" and **"No"**

The decision by the simple majority: 50%+1

Let Verifier perform a series of n challenge-response rounds.

Given that the actual distance $s_1 - s_0 = R + h$,

let $p_n^{\mathtt{error}}(R, h)$ be **the conditional probability** of that

Verifier makes an *erroneous* decision to grant the access because

he has observed "$t_1 - t_0 \leq R$" in more than $\frac{n}{2}$ rounds.

The decision by the simple majority: 50%+1

Let Verifier perform a series of n challenge-response rounds.

Given that the actual distance $s_1 - s_0 = R + h$,

let $p_n^{\text{error}}(R, h)$ be **the conditional probability** of that Verifier makes an *erroneous* decision to grant the access because **he has observed "$t_1 - t_0 \leq R$" in more than $\frac{n}{2}$ rounds.**

Theorem 17.1 **(i)** ***For*** $0 < h \leq \frac{1}{2}$,

$$\lim_{n\to\infty} p_n^{\text{error}}(R, h) = \frac{1}{2}$$

(ii) ***For*** $\frac{1}{2} < h < 1$,

$$p_n^{\text{error}}(R, h) \leq C_0(1 - \delta_h)^n \quad \textit{(for some } \delta_h \textit{ and } C_0\textit{)},$$

and, hence,

$$\lim_{n\to\infty} p_n^{\text{error}}(R, h) = 0.$$

Thm 17.1, What is a secret with $p < \frac{1}{2}$?

Let $p = p_{\mathtt{error}}(R, h)$, $q = 1 - p$, and

$$\alpha_n(p) = p_n^{\mathtt{error}}(R, h).$$

We take the derivative α'_n and compute the ratio, with $n+2$ (sic!):

$$\lim_{n\to\infty} \frac{\alpha'_n(p)}{\alpha'_{n+2}(p)} = 4pq$$

(i) For $0 < h \leq \frac{1}{2}$, we have $p = \frac{1}{2}$, and, hence, $\boxed{4pq = 1}$,
and we have to use **something else** (the harmonic series. . .)

(ii) For $\frac{1}{2} < h < 1$, we have $p < \frac{1}{2}$, and, hence, $\boxed{4pq < 1}$,
which provides that

$$p_n^{\mathtt{error}}(R, h) = \alpha_n(p) \leq C_0(1 - \delta_h)^n.$$

The decision by the larger majority with $c > \frac{1}{2}$

Let Verifier perform a series of n challenge-response rounds.

Let c be a 'threshold number' such that $0.5 < c < 1$.

Given that the actual distance $s_1 - s_0 = R + h$,

let $\pi_n^{\texttt{error}}(R, h)$ be **the conditional probability** of that Verifier makes an *erroneous* decision to grant the access because **he has observed "$t_1 - t_0 \leq R$" at least in cn rounds.**

The decision by the larger majority with $c > \frac{1}{2}$

Let Verifier perform a series of n challenge-response rounds.

Let c be a 'threshold number' such that $0.5 < c < 1$.

Given that the actual distance $s_1 - s_0 = R + h$,

let $\pi_n^{\text{error}}(R, h)$ be **the conditional probability** of that Verifier makes an *erroneous* decision to grant the access because **he has observed "$t_1 - t_0 \leq R$" at least in cn rounds.**

Theorem 19.1 **For all $h > 0$,**

$$\pi_n^{\text{error}}(R, h) \leq C_0(1 - \delta_c)^n \quad \textit{(for some } \delta_c \textit{ and } C_0\textit{)},$$

and, hence,

$$\lim_{n \to \infty} \pi_n^{\text{error}}(R, h) = 0.$$

Thm 19.1, Proof sketch: for $c = \frac{3}{5}$ What is a secret with $p \leq \frac{1}{2}$?

Let $p = p_{\mathtt{error}}(R, h)$, $q = 1 - p$, and

$$\beta_n(p) = \pi_n^{\mathtt{error}}(R, h).$$

We take the derivative β'_n and compute the ratio, with $n+5$ (sic!):

$$\lim_{n\to\infty} \frac{\beta'_n(p)}{\beta'_{n+5}(p)} = \boxed{\frac{5^5}{3^3 \cdot 2^2} p^3 q^2} \leq \frac{5^5}{3^3 \cdot 2^2} \cdot \frac{1}{32} \approx 0.9 < 1$$

which provides that

$$\pi_n^{\mathtt{error}}(R, h) = \beta_n(p) \leq C_0(1 - \delta)^n.$$

The simple majority vs. the larger majority

The "standard thresholds" known in practice are $\frac{2}{3}$ and $\frac{3}{5}$.

Thm 19.1: $\pi_n^{\texttt{error}}(R,h) \le C_0(1-\delta)^n$, for all $h > 0$,

- As a corollary, having observed the event

  $$\text{“}t_1 - t_0 \le R\text{”}$$

  at least in the **60% majority** of rounds, Verifier can establish that *the actual distance is correct* (modulo infinitesimals ε):

  $$s_1 - s_0 \le R + \varepsilon,$$

  but only *with the high probability for large* $n \ge n_0$.

- If Verifier decides to grant the access by the *large majority* with *a fixed threshold* $c > \frac{1}{2}$, then in-between-ticks attacks can be **ruled out with high probability for large** n.

Concluding Remarks: The general method to investigate a wide class of novel security problems

Traditionally, any attack is classified

1. either as the "**must-be**" attack that always succeeds under the given circumstances, "*the probability is* 1"
2. or as the "**may-be**" attack that can succeed sometimes, in the case of a specific scenario, "*the probability is non-zero*"

The novelty of our approach is that we have investigated the case in between these two ends on the scale. Namely,
the attack can succeed but with a certain probability.

1. The probabilistic analysis of an attack on Distance-Bounding Protocols

For a typical challenge-response protocol we have given the full probabilistic analysis of **the attack in between ticks** (and its **variations**) established by Kanovich, Kirigin, Nigam, Scedrov, and Talcott [POST 2015].

(a) We have measured the **probabilistic discrepancy** between the *measured* time distance $t_1 - t_0$, and the *actual* time distance $s_1 - s_0$.

(b) We have found that such discrepancy is caused by **inconsistency** between *the continuous time in nature* and *the discrete time within Verifier's computer clock*.

2. Can we mitigate or even rule out the attacks by using challenge-response rounds repeatedly ?

Within the precise formalism, we *have challenged a general belief* that Verifier can improve their performance by observing the "acceptance events" in *the majority of n rounds*.

(1) If the distance bounding step measurement is repeated n times, and Verifier determines that Prover is within a certain distance, R, in *more than $\frac{n}{2}$ of the cases*, then this information is **still insufficient to mitigate** in-between-ticks attacks.

(2) If Verifier determines that Prover is within a certain distance *in cn of the cases*, with $0.5 < c < 1$, then in-between-ticks attacks can be **ruled out with high probability for large n**.

Thanks ! Questions ? Variations ?

Variations in

- questions (Yes/No issues), models, bounds (a non-integer R), etc.

Upon request, if time allows, the secrets of the proofs for

- Thm 12.1 on:
  $p_{\texttt{error}}(R, h)$, **the probability of the erroneous decision**

- Thm 17.1 on: **the simple majority**

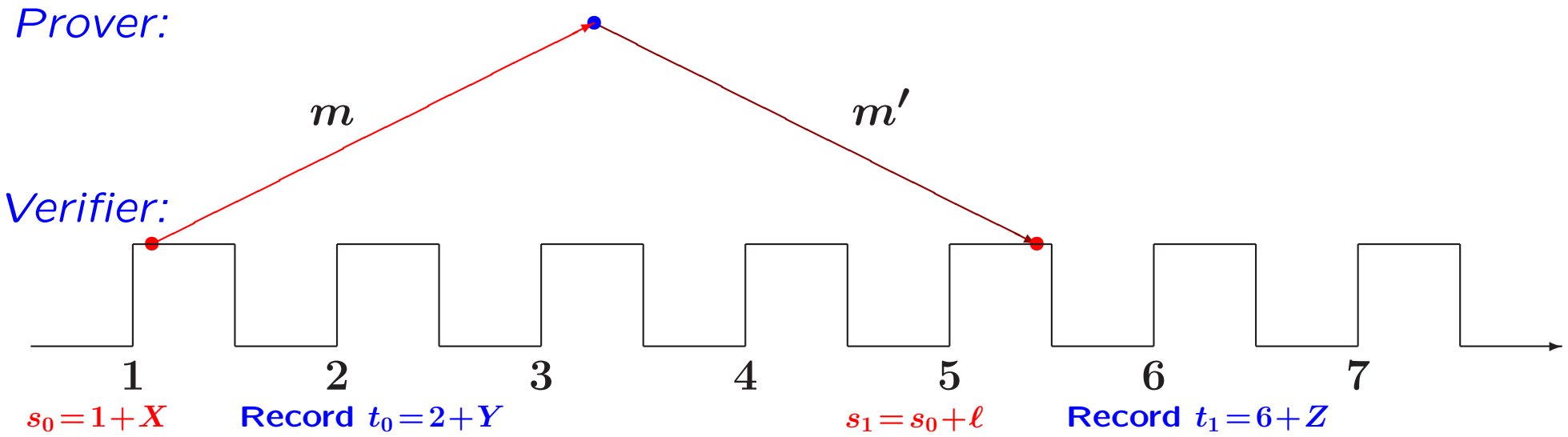
- Thm 19.1 on: **the $\frac{3}{5}$ majority**

"Doing nothing makes no mistakes" Symmetrical "Yes/NO" issues to be addressed.

- **The "Yes" decision** (caused by the *measured* $t_1 - t_0 \leq R$) is taken as **erroneous**, if in reality the *actual distance*, $s_1 - s_0$, turns out to be larger than R, by some positive *excess/extra*, h.

- However, caused by the *measured* $t_1 - t_0 > R + \delta$, **the "NO" decision** should have been taken as **erroneous** as well, if in reality the honest Prover has happened in the appropriate proximity to Verifier.

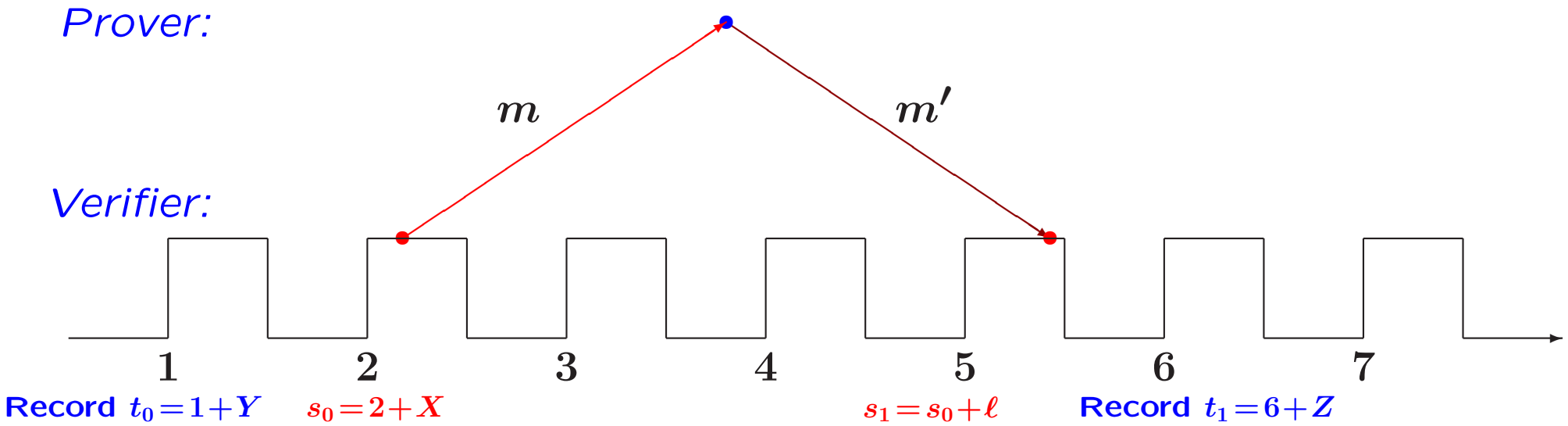
The original challenge-response protocol "t_0 after s_0"



$$\begin{cases} s_0 = 1 + X, & s_1 = s_0 + \ell, \\ t_0 = 2 + Y, & t_1 = \lfloor s_1 \rfloor + 1 + Z. \end{cases}$$

X, Y, and Z are distributed on $[0, \frac{1}{2}]$.

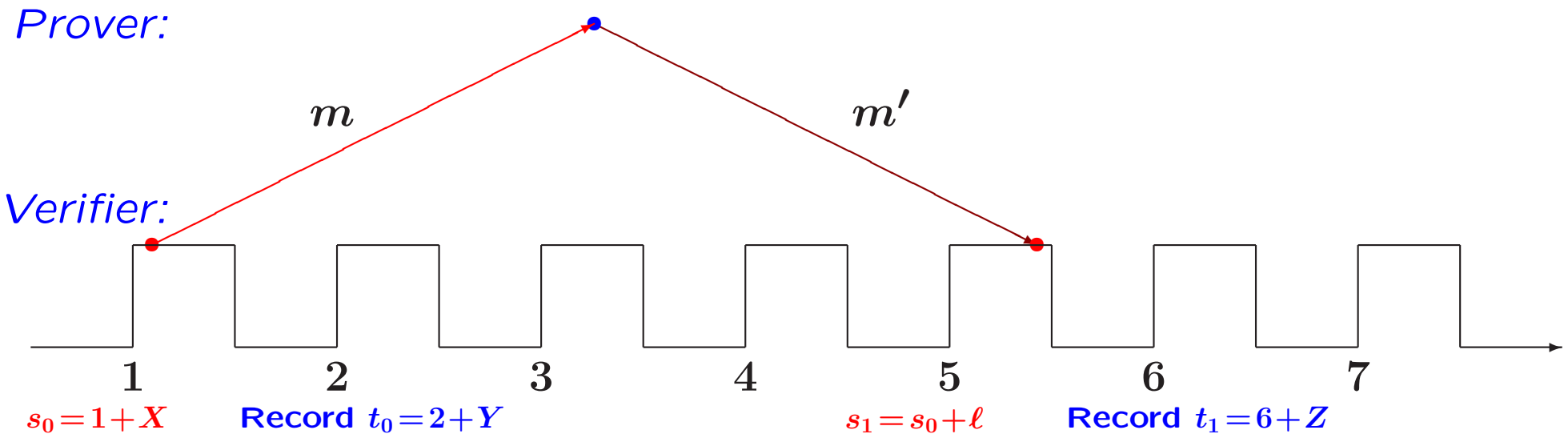
The challenge-response protocols
Variations: "t_0 before s_0"



$$\begin{cases} s_0 = 2 + X, & s_1 = s_0 + \ell, \\ t_0 = 1 + Y, & t_1 = \lfloor s_1 \rfloor + 1 + Z. \end{cases}$$

X, Y, and Z are distributed on $[0, \frac{1}{2}]$.

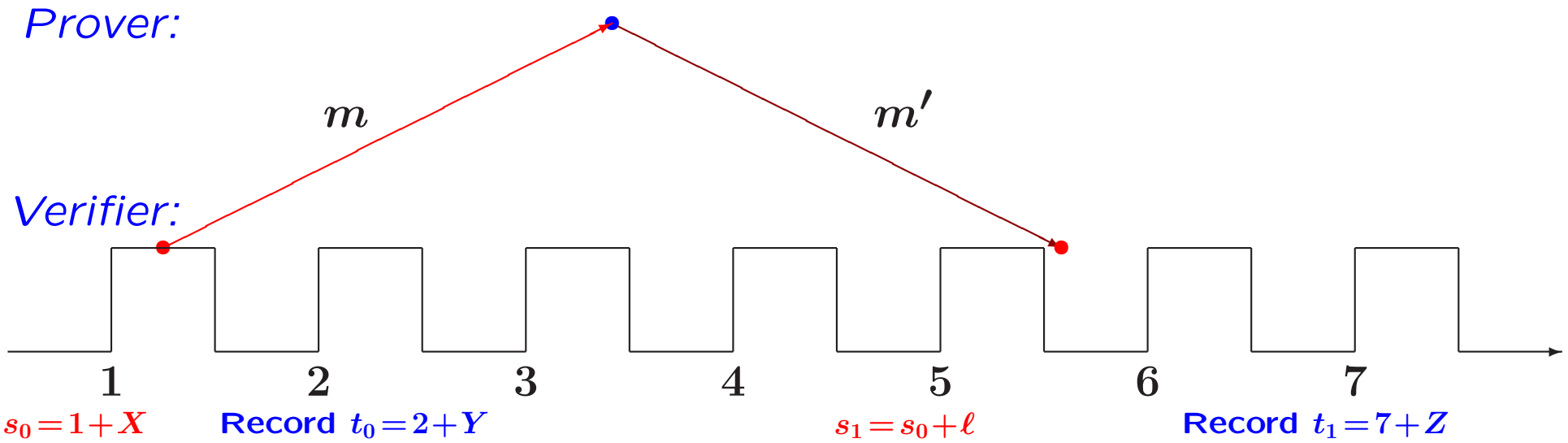
The original challenge-response protocol



$$\begin{cases} s_0 = 1 + X, & s_1 = s_0 + \ell, \\ t_0 = 2 + Y, & t_1 = \lfloor s_1 \rfloor + 1 + Z. \end{cases}$$

X, Y, and Z are distributed on $[0, \frac{1}{2}]$.

The challenge-response protocols (variations): adjust t_1 for s_1 *during the idle half of the cycle*



$$\begin{cases} s_0 = 1 + X, & s_1 = s_0 + \ell, \\ t_0 = 2 + Y, & t_1 = \lceil s_1 + \frac{1}{2} \rceil + Z \ . \end{cases}$$

X, Y, and Z are distributed on $[0, \frac{1}{2}]$.

The probability of the erroneous decision

$$\begin{cases} \mathrm{s}_0 = 1 + \mathrm{X}, & \mathrm{s}_1 = \mathrm{s}_0 + \ell, \\ t_0 = 2 + Y, & t_1 = \lceil s_1 + \frac{1}{2} \rceil + Z \ . \end{cases}$$

Theorem 31.1

Let Y ***and*** Z ***be distributed with one and the same density,*** *an arbitrary* g.

Let X ***be uniformly distributed on*** $[0, \frac{1}{2}]$.

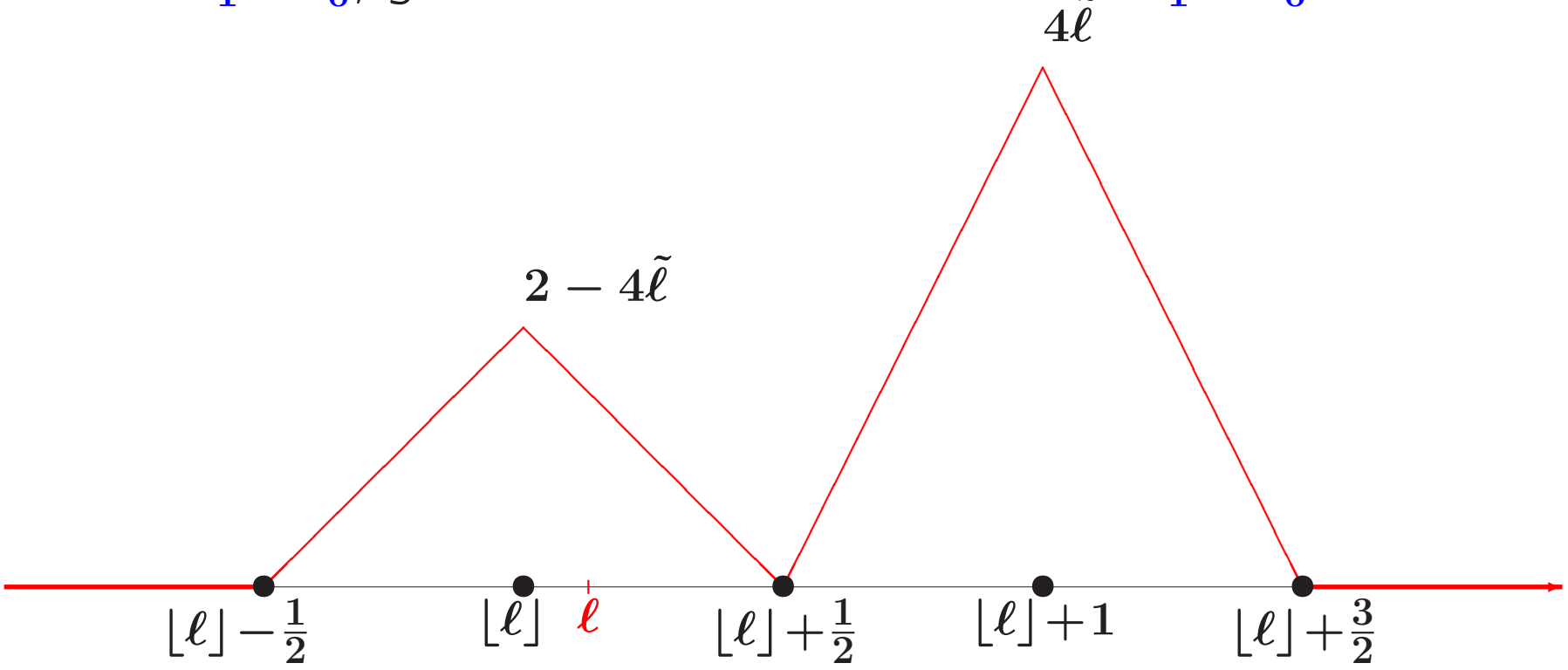
Then, for a fixed time response bound, **an integer** R, ***and an extra,*** **a positive** h,

$$p_{\mathtt{error}}(R, h) = \begin{cases} \frac{1}{2} - h, & \textit{if } 0 < h \leq \frac{1}{2}, \\ 0, & \textit{if } h > \frac{1}{2}. \end{cases} \qquad (3)$$

The 2-humped Bactrian camel: $\tilde{\ell} = \ell - \lfloor \ell \rfloor < \frac{1}{2}$. A bimodal distribution

$$\frac{d}{dw} \mathtt{Prob}\{\, t_1 - t_0 \leq w \mid s_1 - s_0 = \ell \,\}$$

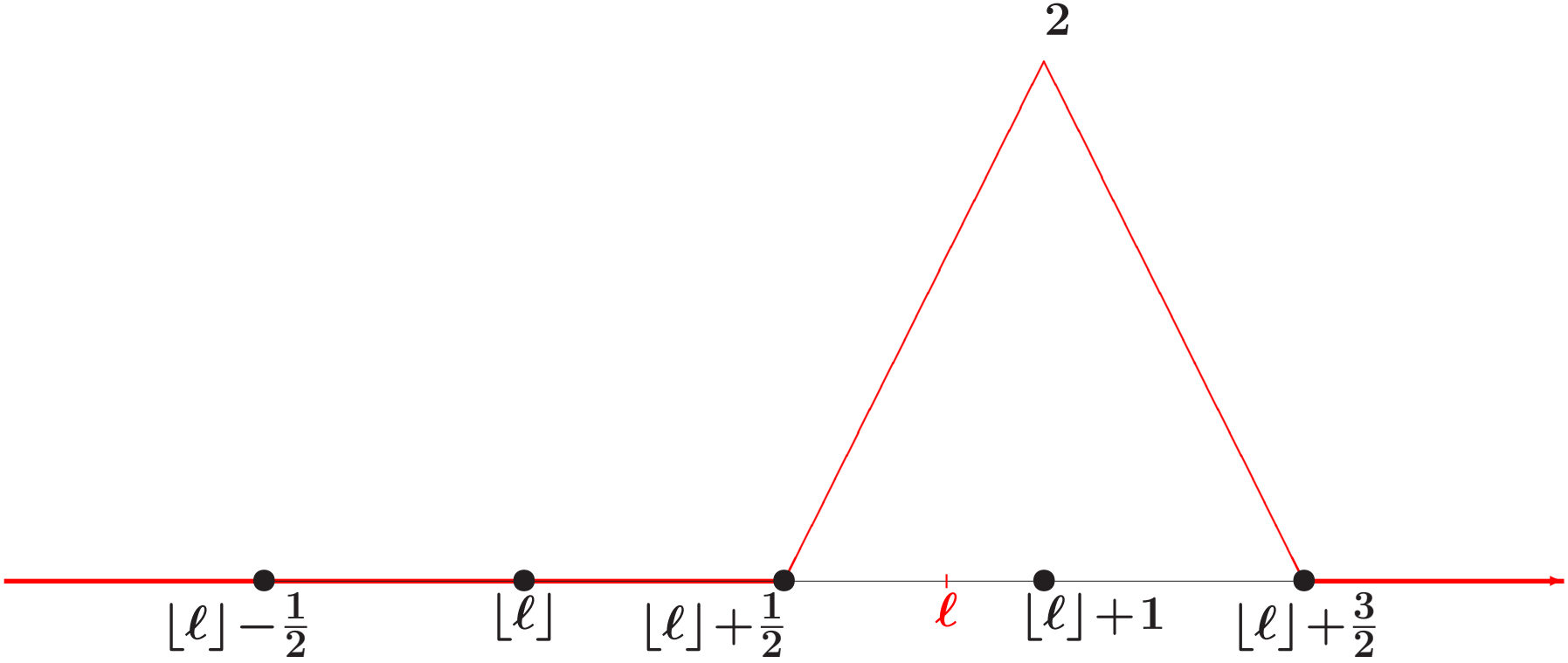
The conditional probability density of the *measured* time distance $t_1 - t_0$, given the *actual* time distance $s_1 - s_0 = \ell$:



The single-humped Dromedary: $\tilde{\ell} = \ell - \lfloor \ell \rfloor \geq \frac{1}{2}$.

$$\frac{d}{dw} \mathtt{Prob}\{ t_1 - t_0 \leq w \mid s_1 - s_0 = \ell \}$$

The conditional probability density of the *measured* time distance $t_1 - t_0$, given the *actual* time distance $s_1 - s_0 = \ell$:



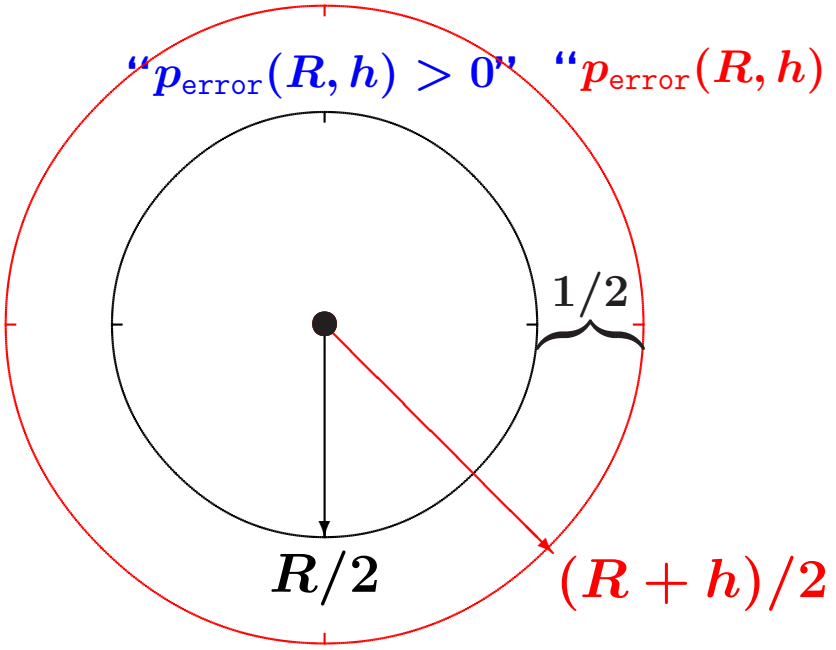
Thanks ! Questions ?

Proofs for Thm 12.1: $p_{\mathtt{error}}(R, h)$; Thm 17.1: $50\% + 1$; Thm 19.1: 60%;

Proofs for:

- Thm 12.1 on:
  $p_{\mathtt{error}}(R, h)$, **the probability of the erroneous decision**
- Thm 17.1 on: **the simple majority**
- Thm 19.1 on: **the $\frac{3}{5}$ majority**

The probability of the erroneous decision (Thm 12.1, R is an integer)

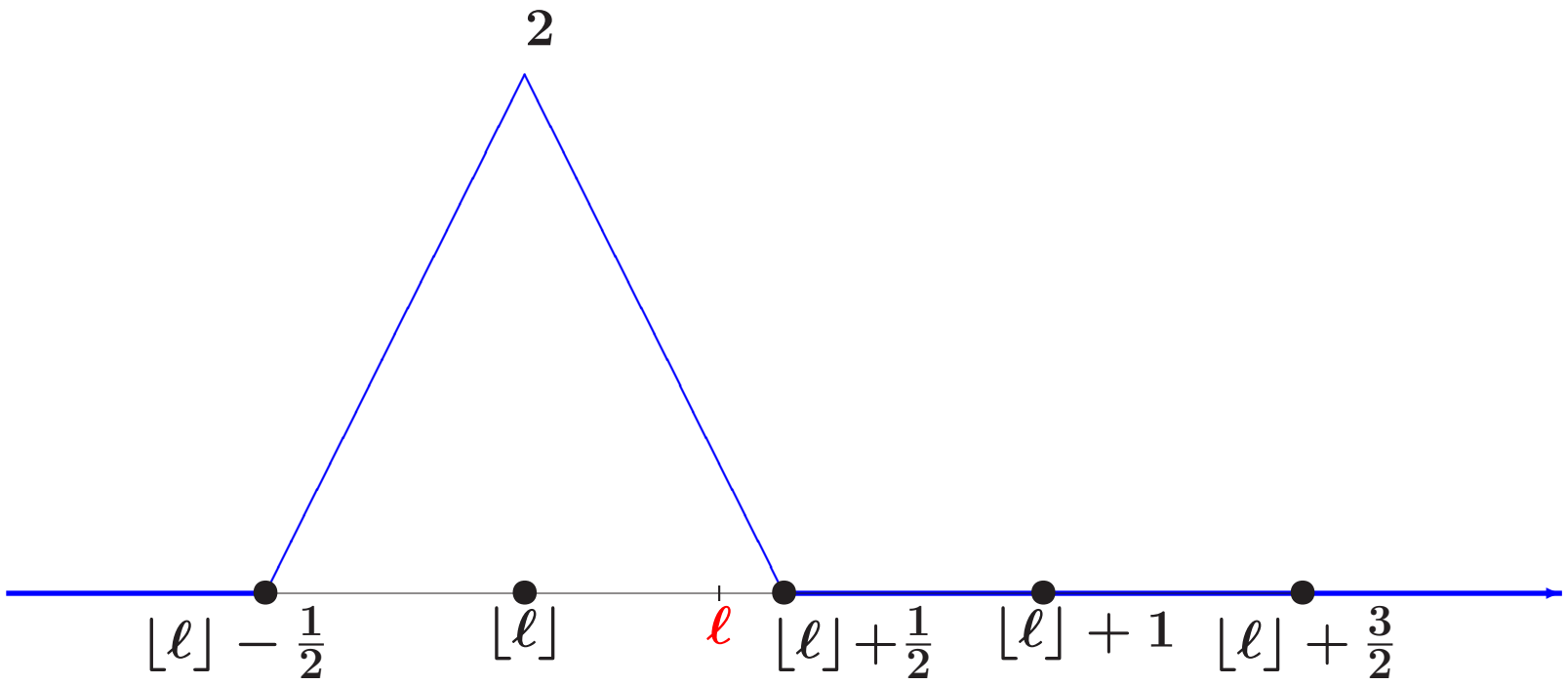


$$p_{\mathrm{error}}(R,h) = \begin{cases} \frac{1}{2}, & \text{if } 0 < h \le \frac{1}{2}, \\ 1-h, & \text{if } \frac{1}{2} < h < 1, \\ 0, & \text{if } h \ge 1. \end{cases}$$

("Dromedary camel" case) $\widetilde{\ell} = \ell - \lfloor \ell \rfloor \leq \frac{1}{2}$.

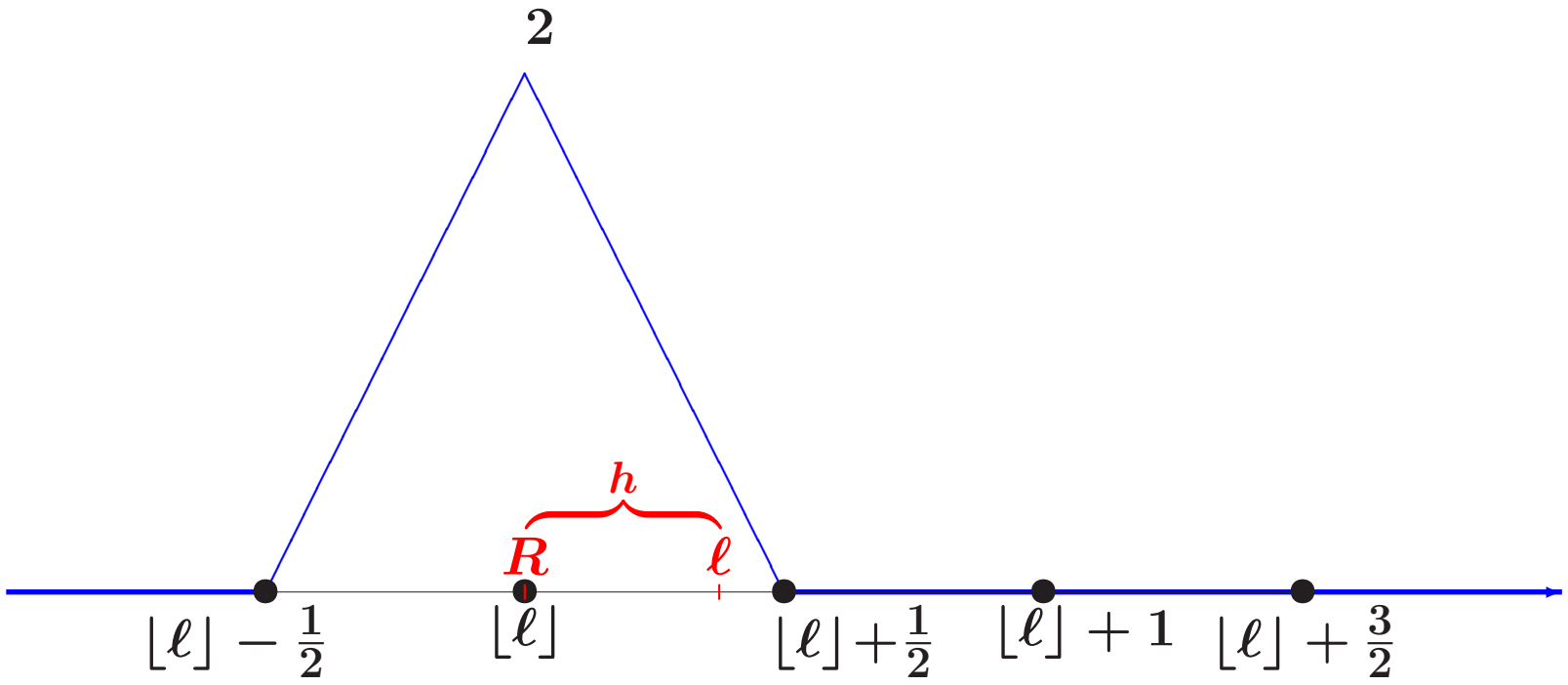
The graph of the density, $F'_\ell(w)$, for the distribution $F_\ell(w)$:

$$F_\ell(w) = \texttt{Prob}\{\ t_1 - t_0 \leq w \mid s_1 - s_0 = \ell\ \}$$



$F'_\ell(w)$ is always 'symmetrical' whenever $f_Y = f_Z$.

Thm 12.1, Proof: $p_{\texttt{error}}(R,h) = \frac{1}{2}$, if $0 < h \leq \frac{1}{2}$



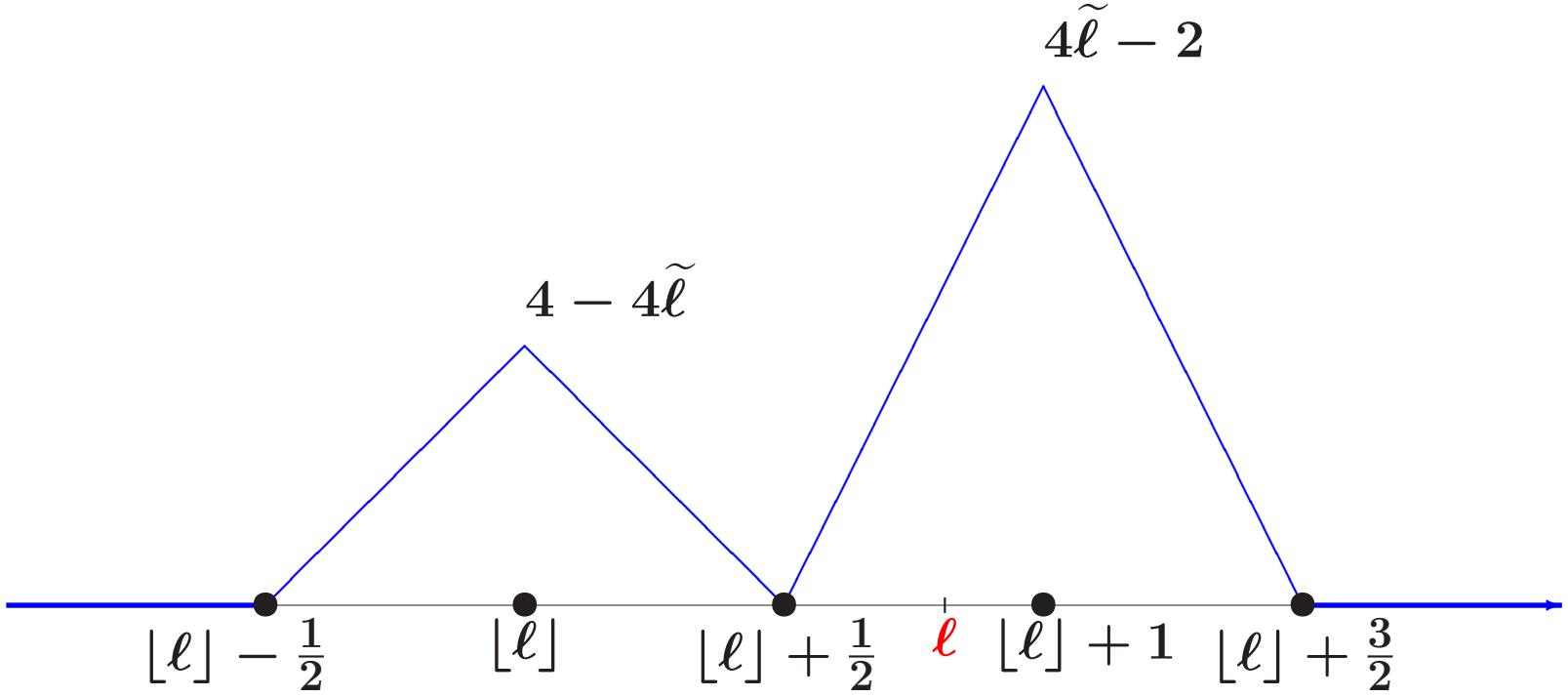
Given an integer R, let $\ell = R + h$. Then $\lfloor \ell \rfloor = R$, and

$$p_{\texttt{error}}(R,h) = \int_{-\infty}^{\lfloor \ell \rfloor} F'_{\ell}(w)\, dw = \frac{1}{2}$$

("Bactrian camel" case) $\widetilde{\ell} = \ell - \lfloor \ell \rfloor > \frac{1}{2}$

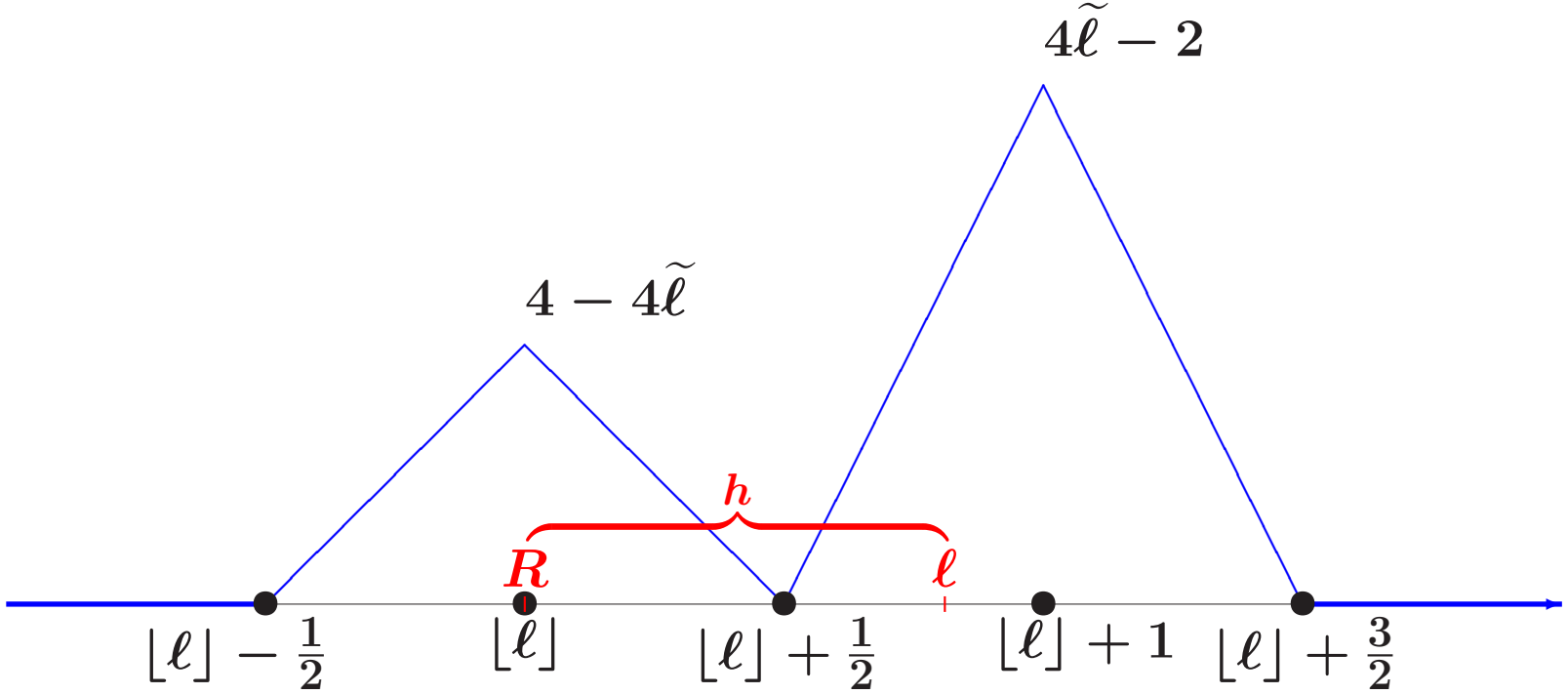
The graph of the density, $F'_\ell(w)$, for the distribution $F_\ell(w)$:

$$F_\ell(w) = \texttt{Prob}\{\ t_1 - t_0 \le w \mid s_1 - s_0 = \ell\ \}$$



$F'_\ell(w)$ is always 'symmetrical' whenever $f_Y = f_Z$.

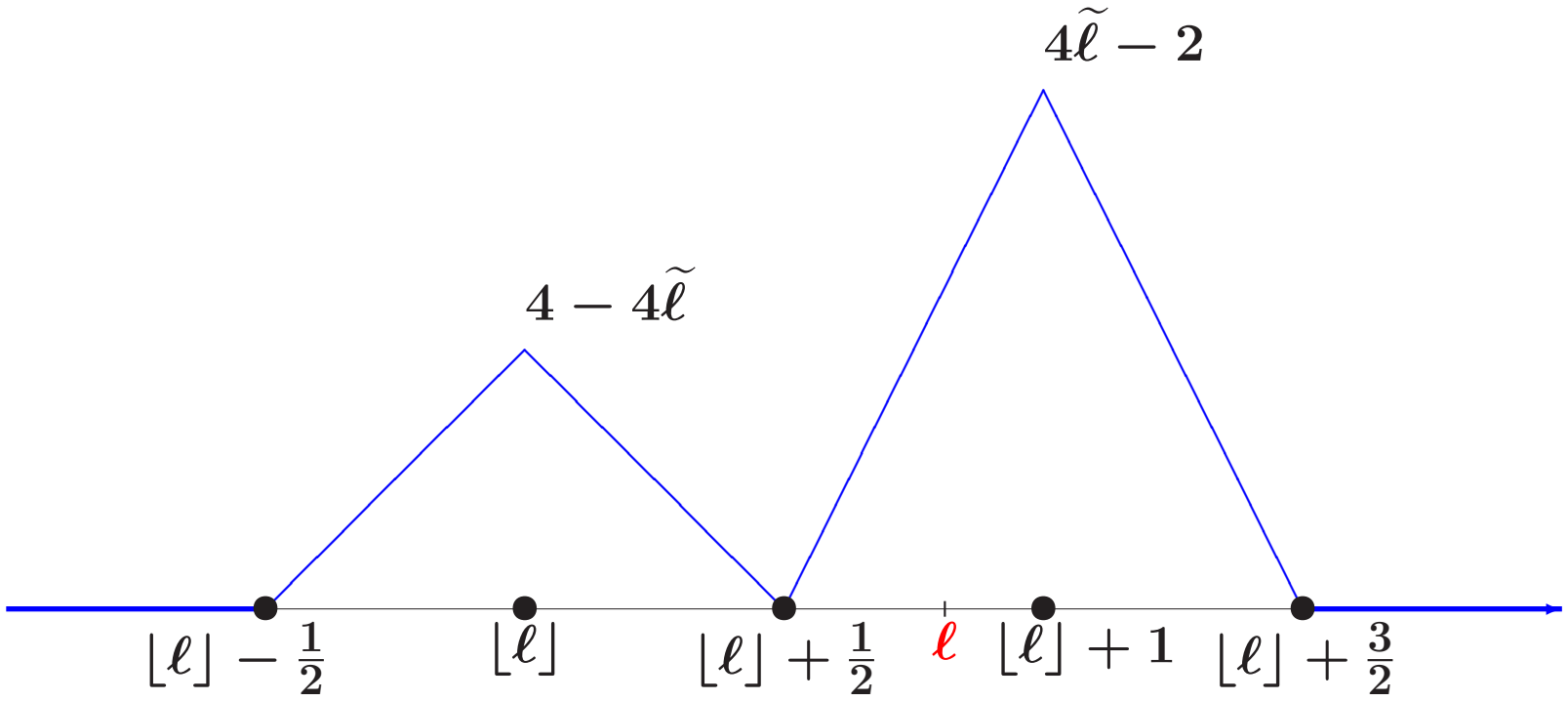
Thm 12.1, Proof: $p_{\text{error}}(R,h) = 1-h$, if $\frac{1}{2} < h < 1$



Given an integer R, let $\ell = R + h$. Then $\lfloor \ell \rfloor = R$, and

$$p_{\text{error}}(R,h) = \int_{-\infty}^{\lfloor \ell \rfloor} F'_{\ell}(w)\, dw = 1 - \widetilde{\ell} = 1 - h$$

Thm 12.1, Proof: $p_{\texttt{error}}(R,h) = 0$, if $h \geq 1$



Given an integer R, let $\ell = R + h$. Then $R \leq \lfloor \ell \rfloor - 1$, and

$$p_{\texttt{error}}(R,h) \leq \int_{-\infty}^{\lfloor \ell \rfloor - 1} F'_\ell(w)dw = 0.$$

Thm 17.1: The decision by the simple majority

Let Verifier perform a series of n challenge-response rounds.
Let $p_n^{\text{error}}(R,h)$ be the conditional probability of that, given that the actual time distance

$$s_1 - s_0 = R + h,$$

Verifier makes an erroneous decision to grant the access because he has observed an event "$t_1 - t_0 \le R$" in *more than* $\frac{n}{2}$ *rounds*.

Thm 17.1.
(i) For $0 < h \le \frac{1}{2}$,

$$\lim_{n\to\infty} p_n^{\text{error}}(R,h) = \frac{1}{2} = p_1^{\text{error}}(R,h)$$

(ii) For $\frac{1}{2} < h < 1$, **for some positive** δ_h **and** C_0,

$$p_n^{\text{error}}(R,h) \le C_0(1-\delta_h)^n$$

and, hence,

$$\lim_{n\to\infty} p_n^{\text{error}}(R,h) = 0.$$

Thm 17.1, Proof sketch

Given $p = p_{\mathtt{error}}(R, h)$ and $q = 1 - p$,

$$f_{n,k}(p) = p^n + np^{n-1}q + \cdots + \binom{n}{k} p^{n-k}q^k$$

is the conditional probability of that, given that the actual

$$s_1 - s_0 = R + h,$$

Verifier has observed an event of the 'non-acceptance form' **"$t_1 - t_0 > R$" in no more than k rounds**.

$$\underbrace{\text{Yes} \quad \text{Yes} \quad \ldots \quad \text{Yes}}_{n-k \text{ times, or more}} \quad \underbrace{\text{No} \quad \text{No} \quad \ldots \quad \text{No}}_{\mathtt{k} \text{ times, or less}}$$

E.g., we express the *simple majority* by $n - k > \frac{n}{2}$.
If we denote $\alpha_n(p) = p_n^{\mathtt{error}}(R, h)$, then, with $k = \lceil \frac{n}{2} \rceil - 1$,

$$p_n^{\mathtt{error}}(R, h) = f_{n,k}(p) = \alpha_n(p).$$

Thm 17.1, Proof sketch for $0 < h \leq \frac{1}{2}$

For $0 < h \leq \frac{1}{2}$, we have

$$p = p_{\texttt{error}}(R, h) = \frac{1}{2} = q,$$

and

$$\lim_{n \to \infty} p_n^{\texttt{error}}(R, h) = \lim_{n \to \infty} \alpha_n(0.5) = \frac{1}{2}$$

The latter is a quite non-trivial fact with invoking the harmonic series.

Thm 17.1, Proof sketch for $\frac{1}{2} < h < 1$

Here $p = p_{\mathtt{error}}(R, h) = 1 - h < \frac{1}{2}$.

We take the derivative α'_n

$$\alpha'_n(p) = \frac{df_{n,k}}{dp}(p) = \frac{n!}{k!\,(n-k-1)!}\,p^{n-k-1}q^k$$

and compute the ratio, with $n+2$ (sic!):

$$\lim_{n\to\infty} \frac{\alpha'_n(p)}{\alpha'_{n+2}(p)} = 4pq < 1.$$

The effect is that, for some positive δ_p and C_0,

$$\alpha'_n(p') \le C_0(1-\delta_p)^n, \text{ for all } 0 \le p' \le p < \tfrac{1}{2}.$$

Hence, taking into account that $\alpha_n(0) = 0$,

$$p_n^{\mathtt{error}}(R, h) = \alpha_n(p) = \int_0^p \alpha'_n(p')\,dp' \le C_0(1-\delta_h)^n.$$

and

$$\lim_{n\to\infty} p_n^{\mathtt{error}}(R, h) = 0.$$

The decision by the larger majority with $c > \frac{1}{2}$

Let Verifier perform a series of n challenge-response rounds.

Let c be a 'threshold number' such that $0.5 < c < 1$.

Given that the actual distance $s_1 - s_0 = R + h$,

let $\pi_n^{\text{error}}(R, h)$ be **the conditional probability** of that Verifier makes an *erroneous* decision to grant the access because **he has observed "$t_1 - t_0 \leq R$" at least in cn rounds.**

Thm 19.1. For some positive δ_c and C_0,

$$\pi_n^{\text{error}}(R, h) \leq C_0(1 - \delta_c)^n$$

and, hence,

$$\lim_{n \to \infty} \pi_n^{\text{error}}(R, h) = 0.$$

Proof. For the sake of perspicuity, we take $c = \frac{3}{5}$. ∎

Thm 19.1, Proof sketch: for $c = \frac{3}{5}$

Here $p = p_{\text{error}}(R, h) \leq \frac{1}{2}$.

$$f_{n,k}(p) = p^n + np^{n-1}q + \cdots + \binom{n}{k} p^{n-k}q^k$$

is the conditional probability of that, given that the actual distance $s_1 - s_0 = R + h$, Verifier has observed an event of the 'non-acceptance form' **"$t_1 - t_0 > R$" in no more than k rounds**.

$$\underbrace{\text{Yes} \quad \text{Yes} \quad \ldots \quad \text{Yes}}_{n-k \text{ times, or more}} \quad \underbrace{\text{No} \quad \text{No} \quad \ldots \quad \text{No}}_{\text{k times, or less}}$$

We express the *larger majority* by $n - k \geq \frac{3n}{5}$.
If we denote $\beta_n(p) = \pi_n^{\text{error}}(R, h)$, then, with $k = \lfloor \frac{2n}{5} \rfloor$,

$$\pi_n^{\text{error}}(R, h) = f_{n,k}(p) = \beta_n(p).$$

Thm 19.1, Proof sketch, for $c = \frac{3}{5}$ (cont.)

We take the derivative β'_n and compute the ratio, with $n+5$ (sic!):

$$\lim_{n\to\infty} \frac{\beta'_n(p)}{\beta'_{n+5}(p)} = \frac{5^5}{3^3 \cdot 2^2} p^3 q^2 < 1$$

The effect is that, for some positive δ and C_0,

$$\beta'_n(p') \le C_0(1-\delta)^n, \text{ for all } 0 \le p' \le \tfrac{1}{2}.$$

Hence, taking into account that $\beta_n(0) = 0$,

$$\pi_n^{\text{error}}(R,h) = \beta_n(p) = \int_0^p \beta'_n(p')\,dp' \le C_0(1-\delta)^n.$$

and

$$\lim_{n\to\infty} \pi_n^{\text{error}}(R,h) = 0.$$

Thanks

Distance-Bounding Protocols

[1] D. A. Basin, S. Capkun, P. Schaller, and B. Schmidt. Formal reasoning about physical properties of security protocols. ACM Trans. Inf. Syst. Secur., 14(2):16, 2011.

[2] **S. Brands and D. Chaum. Distance-bounding protocols (extended abstract). In EUROCRYPT, pages 344-359, 1993.**

[3] S. Capkun and J.-P. Hubaux. Secure positioning in wireless networks. IEEE Journal on Selected Areas in Communications, 24(2):221-232, 2006.

[4] S. Ganeriwal, C. PĄöpper, S. Capkun, and M. B. Srivastava. Secure time synchronization in sensor networks. ACM Trans. Inf. Syst. Secur., 11(4), 2008.

[5] M. Kanovich, T. B. Kirigin, V. Nigam, A. Scedrov, and C. Talcott. Discrete vs. dense times in the analysis of cyber-physical security protocols. In Principles of Security and Trust - 4th International Conference, POST, pages 259-279, 2015.

[6] C. Meadows, R. Poovendran, D. Pavlovic, L. Chang, and P. F. Syverson. Distance bounding protocols: Authentication logic analysis and collusion attacks. In Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks, pages 279-298. 2007.

[7] V. Shmatikov and M.-H. Wang. Secure verification of location claims with simultaneous distance modification. In ASIAN, pages 181-195, 2007.

[8] K. Sun, P. Ning, and C. Wang. Tinysersync: secure and resilient time synchronization in wireless sensor networks. In ACM Conference on Computer and Communications Security, pages 264-277, 2006.

[9] N. O. Tippenhauer and S. Capkun. Id-based secure distance bounding and localization.

In ESORICS, pages 621-636, 2009.