An Efficient Mitigation Method for Timing Side Channels on the Web

Sebastian Schinzel

Friedrich-Alexander Universität Erlangen-Nürnberg

Lehrstuhl für Informatik 1

IT-Sicherheitsinfrastrukturen

Supported by Deutsche Forschungsgemeinschaft (DFG) as part of SPP 1496

“Reliably Secure Software Systems”

Friedrich-Alexander-Universität Erlangen-Nürnberg

USIFES

User-centric, Secure Information Flow Management in Enterprise Systems

Agenda

- Side-channels in non-cryptographic processes
- System model
- Types of timing side channel mitigation
  - Fix response times
  - Add random delay
  - Add a Deterministic and Unpredictable Delay (DUDe)

Friedrich-Alexander-Universität Erlangen-Nürnberg

USIFES

Timing Side-Channels on the web

- Side-Channels in non-cryptographic processes
  - Learn what a user types by observing
    - reflections of monitor picture

      [Michael Backes and Markus Dürmuth and Dominique Unruh, Compromising Reflections-or-How to Read LCD Monitors around the Corner, IEEE Symposium on Security and Privacy, pp. 158-169, IEEE Computer Society, 20081
    - inter-packet timing in encrypted SSH session

      [D. X. Song, D. Wagner, and X. Tian, "Timing analysis of keystrokes and SSH timing attacks," in USENIX Security Symposium, 2001]

Timing Side-Channels on the web

- Side-Channels in non-cryptographic processes
  - Learn about the action a user performs on a Web application by observing packet sizes in encrypted Web traffic

[Shuo Chen and Rui Wang 0010 and XiaoFeng Wang and Kehuan Zhang, Side-Channel Leaks in Web Applications: A Reality Today, a Challenge Tomorrow, IEEE Symposium on Security and Privacy, pp. 191-206, IEEE Computer Society, 2010]

Friedrich-Alexander-Universität Erlangen-Nürnberg

USIFES

Timing Side-Channels on the web

- Side-Channels in non-cryptographic processes
  - Example scenario: learn existence of user name from response time of Web application

[E. W. Felten and M. A. Schneider. Timing attacks on web privacy. In SIGSAC: 7th ACM Conference on Computer and Communications Security. ACM SIGSAC, 2000]

[A. Bortz and D. Boneh. Exposing private information by timing web applications. In C. L. Williamson, M. E. Zurko, P. F. Patel-Schneider, and P. J. Shenoy, editors, WWW, pages 621–628. ACM, 2007]

[Y. Nagami, D. Miyamoto, H. Hazeyama, and Y. Kadobayashi. An independent evaluation of web timing attack and its countermeasure. In Third International Conference an Availability, Reliability and Security (ARES), pages 1319–1324. IEEE Computer Society, 2008.]

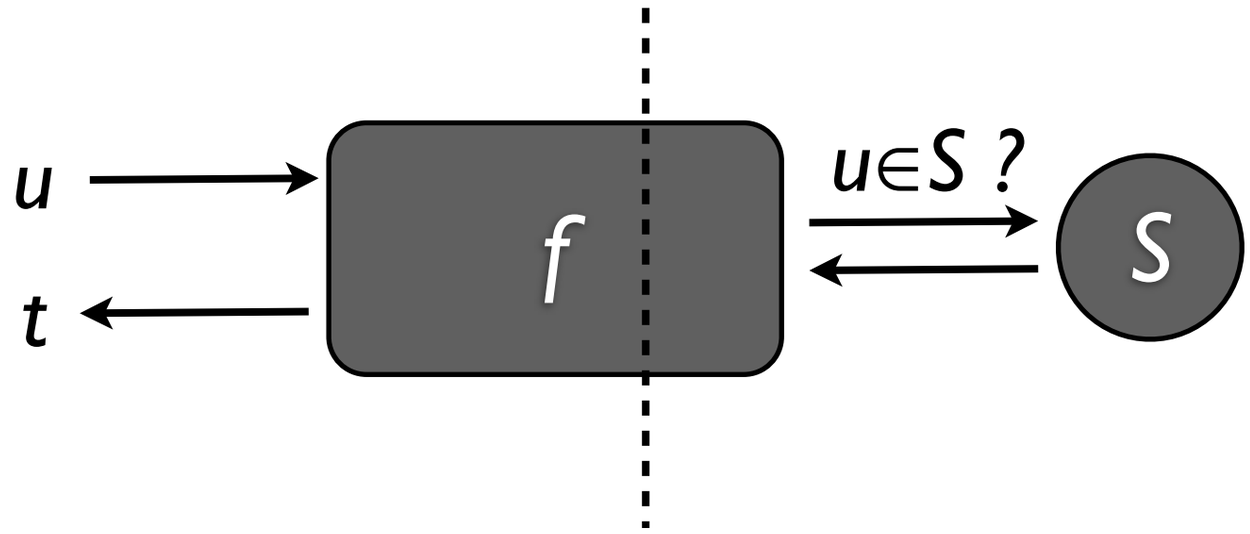
Agenda

- Side-channels in non-cryptographic processes
- System model
- Types of timing side channel mitigation
  - Fix response times
  - Add random delay
  - Add a Deterministic and Unpredictable Delay (DUDe)

Friedrich-Alexander-Universität Erlangen-Nürnberg

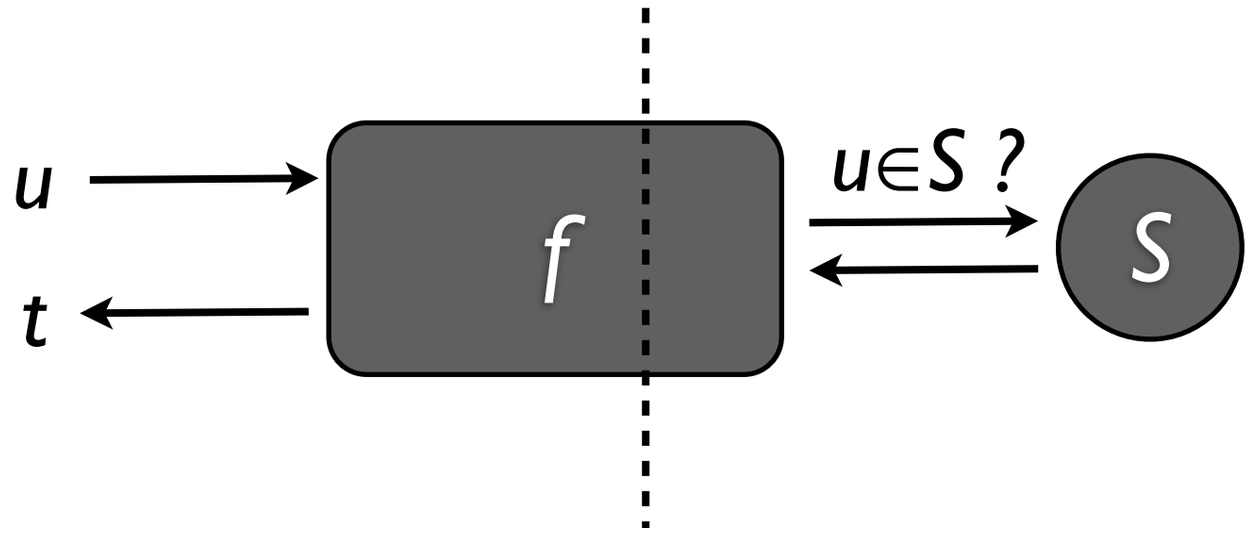
USIFES

System Model



- We model a login process as function $f(U) \rightarrow T$.
- f takes user-chosen value *u∈U and returns timing delay t∈T*
- Assumption: attacker has perfect measurement conditions

System Model



- $S \subset U$ is subset of existing values, $u_a \in S$ and $u_b \notin S$
- *f* forms a timing side channel iff

$$\forall u_a \in S, u_b \notin S : f(u_a) \neq f(u_b)$$

Agenda

- Side-channels in non-cryptographic processes
- System model
- Types of timing side channel mitigation
  - Fix response times
  - Add random delay
  - Add a Deterministic and Unpredictable Delay (DUDe)

Friedrich-Alexander-Universität Erlangen-Nürnberg

USIFES

Types of Mitigation
Fixed response time

- Fix response time to Worst Case Execution Time (WCET)

$t_{delay} = WCET - t_n$

Example:

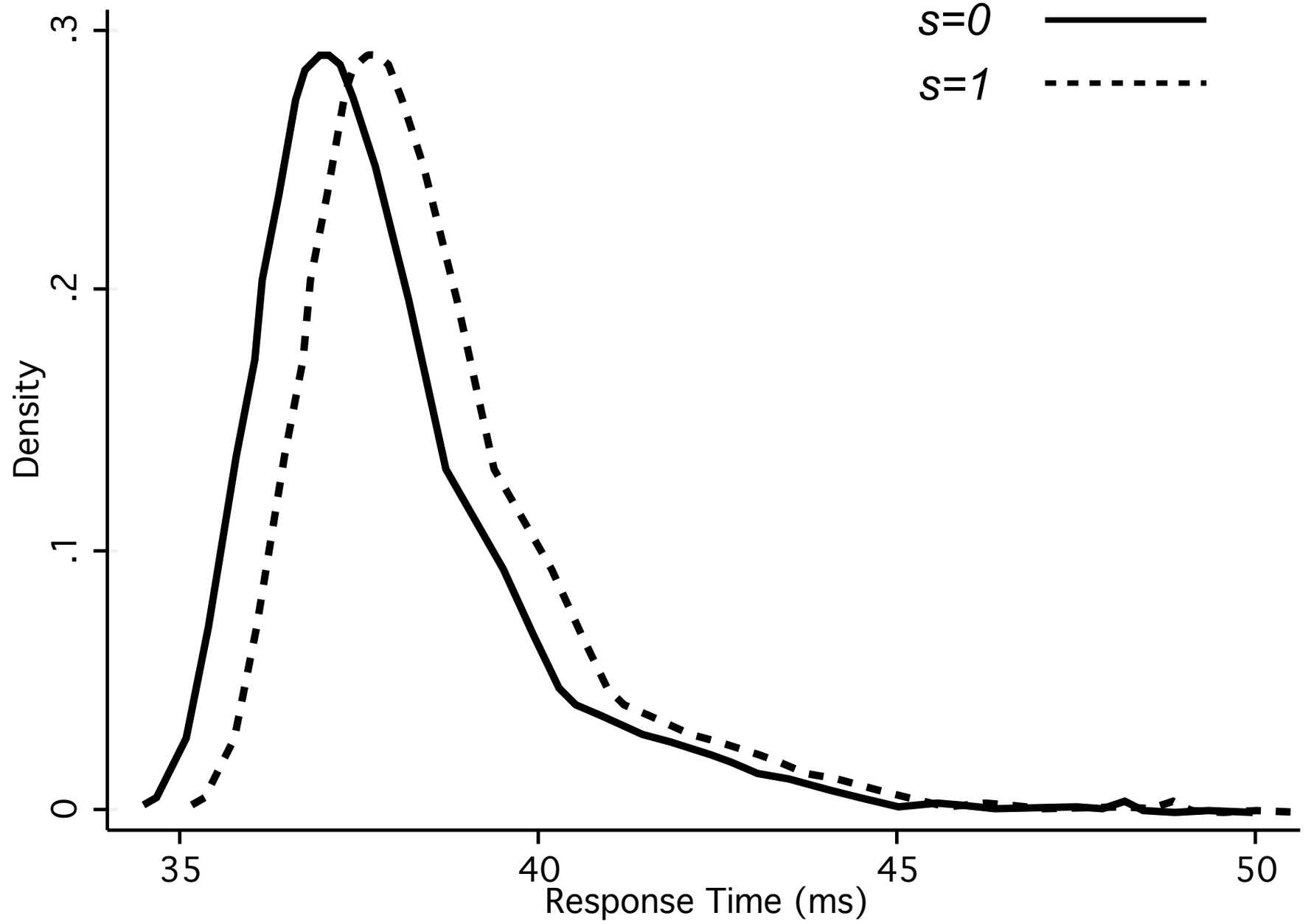
WCET ~ Max(T) = 150 ms

t_1=36,5ms → t_{delay} = 150ms - 36,5ms = 113,5ms

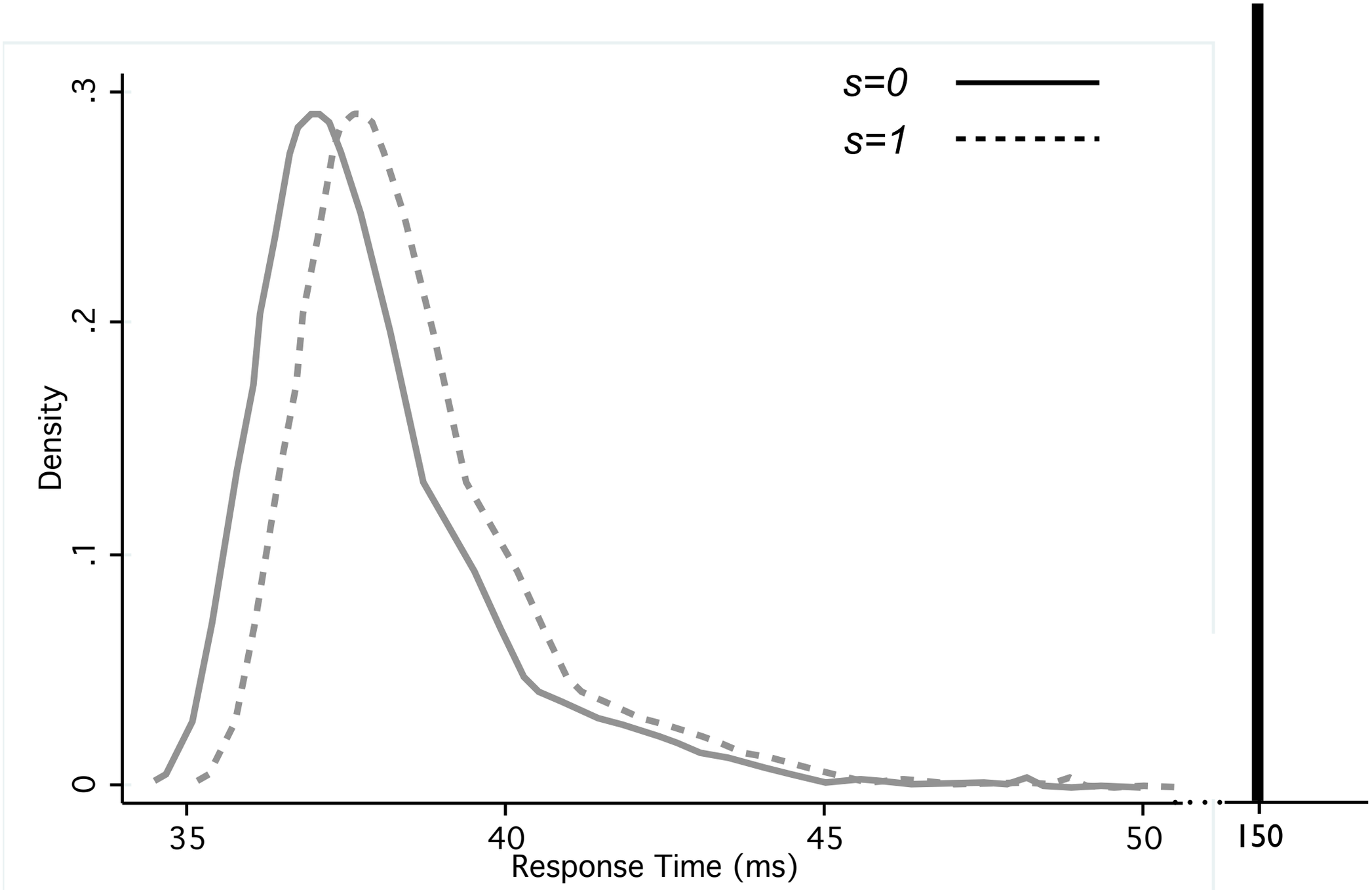
t_2=37,1ms → t_{delay} = 150ms - 37,1ms = 112,9ms

t_3=120,7ms → t_{delay} = 150ms - 120,7ms = 29,3ms

Types of Mitigation
Fixed response time



Types of Mitigation
Fixed response time



Types of Mitigation
Adding a Random Delay

- Add random delay

$t_{delay} = r$ with $r_{min} <= r <= r_{max}$

Example:

$r_{min} = 0ms$, $r_{max} = 30ms$

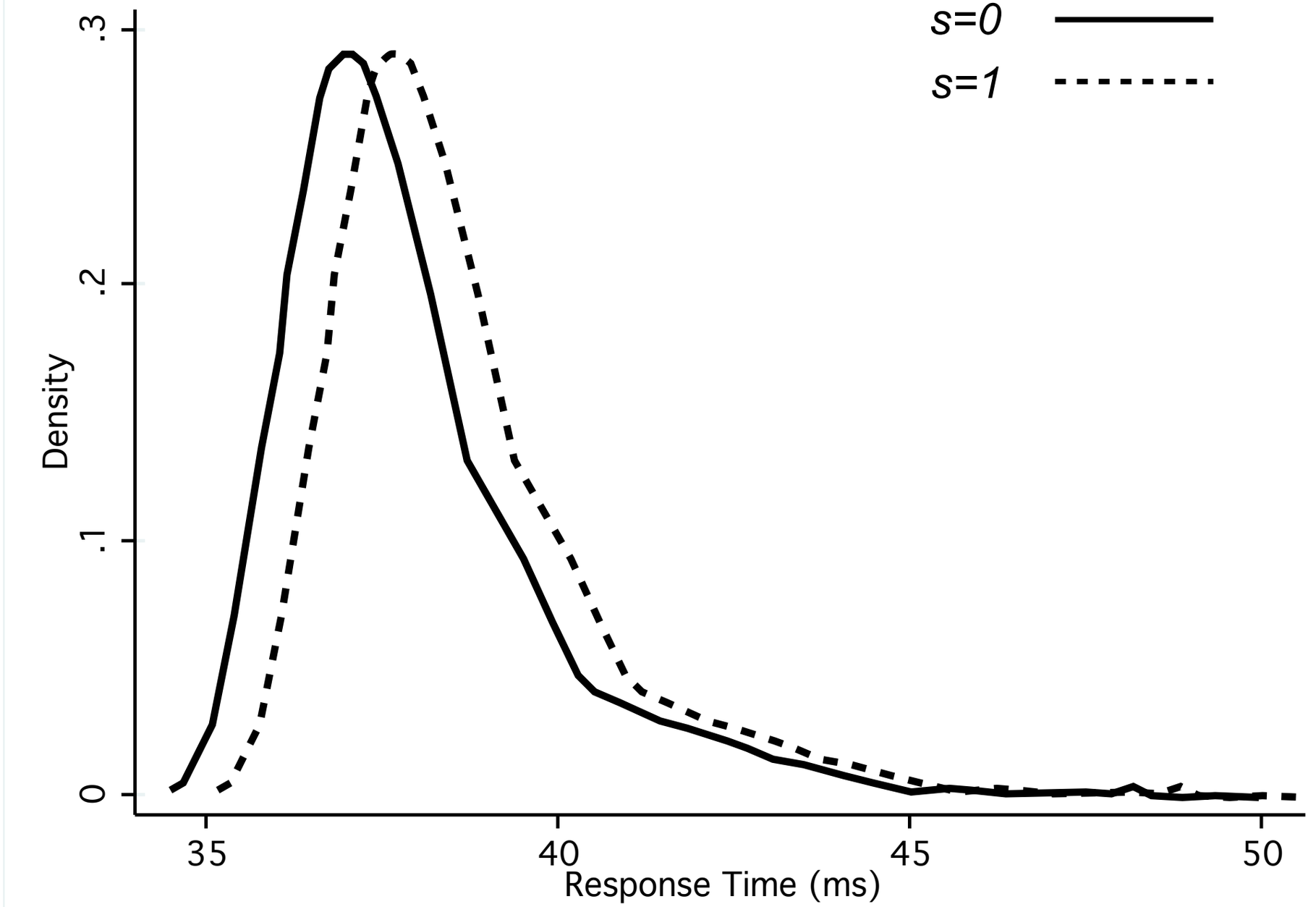
$t_1 = 36,5ms \rightarrow t_{delay} = 23ms \rightarrow t_{ges} = t_1 + t_{delay} = 59,5ms$

$t_2 = 35,9ms \rightarrow t_{delay} = 9ms \rightarrow t_{ges} = t_1 + t_{delay} = 44,9ms$

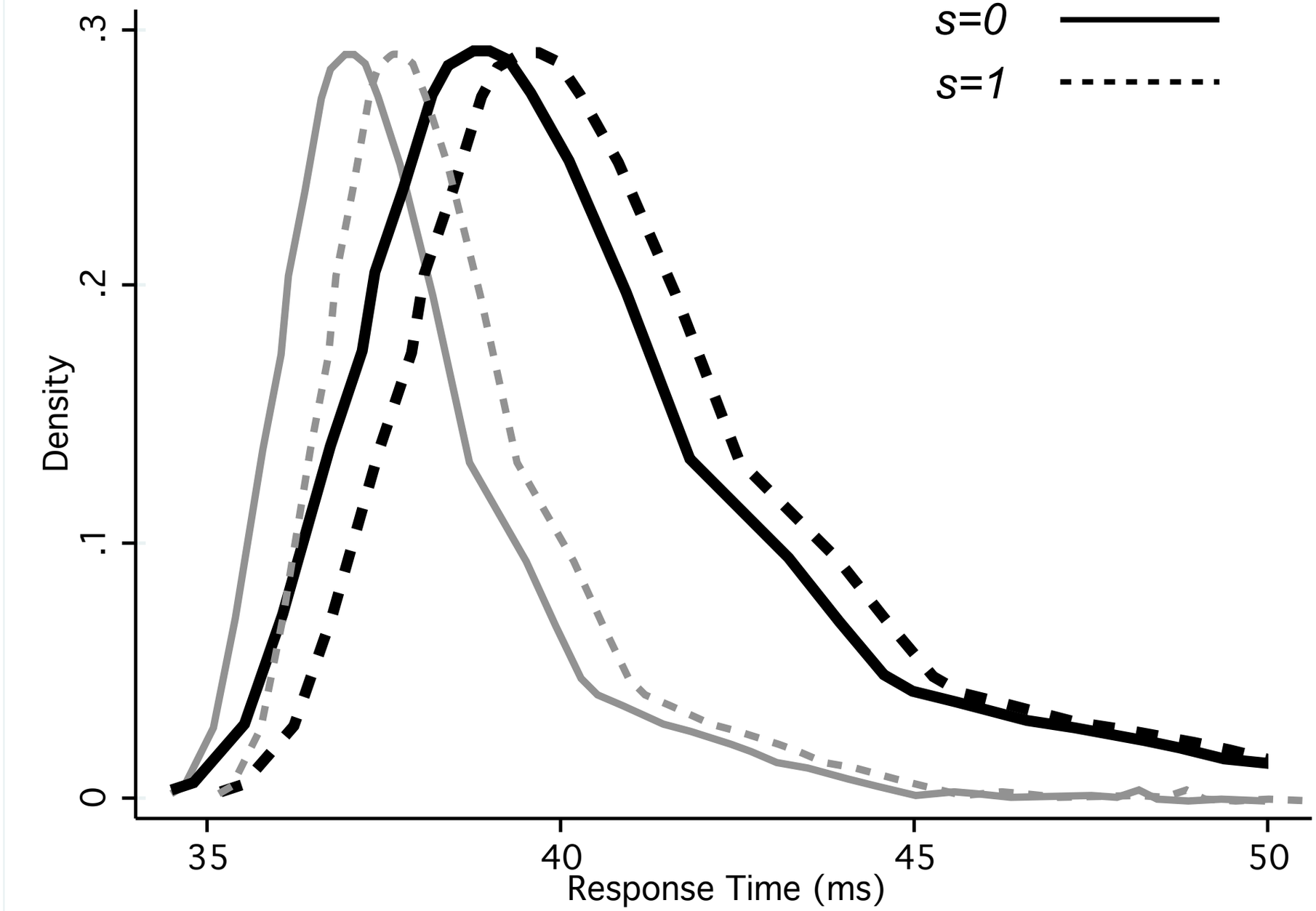
$t_1 = 37,1ms \rightarrow t_{delay} = 11ms \rightarrow t_{ges} = t_1 + t_{delay} = 48,1ms$

- $t_{delay} = WCET - t_n$

Types of Mitigation
Adding a Random Delay



Types of Mitigation
Adding a Random Delay



Types of Mitigation
Adding a Deterministic and Unpredictable Delay

- Add Deterministic and Unpredictable Delay (DUDe)

t_{delay} = $g(i)$ with $g(l) \rightarrow N$ having the requirements:

1. **g is deterministic**
2. **N is uniformly distributed (n_{min} <= n <= n_{max})**
3. **An attacker cannot infer $n \in N$ from any given $i \in I$.**

Implementation example:

```
1 function g(u):
2     k := {secret key unknown to the attacker}
3     t_g := h(u, k) mod t_max
4     sleep_nano_seconds(t_g)
```

Types of Mitigation
Adding a Deterministic and Unpredictable Delay

- Add Deterministic and Unpredictable Delay (DUDe)

Example:

$n_{min} = 0ms, n_{max} = 30ms$

$t_1 = 36,5ms \rightarrow t_{delay} = g(\text{'}\underline{u1}\text{'}, Q) = \underline{19ms} \rightarrow t_{ges} = t_1 + t_{delay} = 55,5ms$

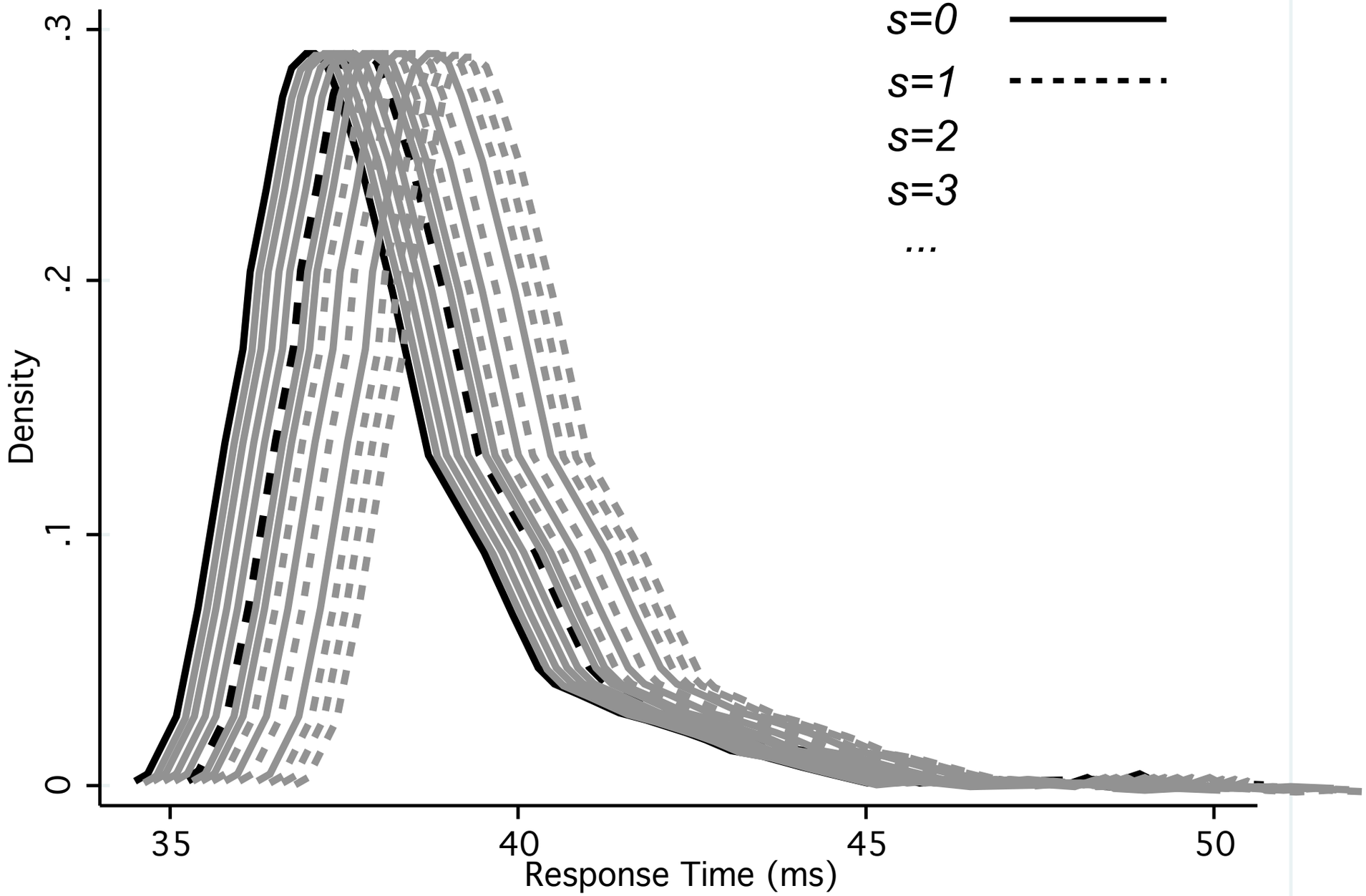
$t_2 = 35,9ms \rightarrow t_{delay} = g(\text{'}\underline{u1}\text{'}, Q) = \underline{19ms} \rightarrow t_{ges} = t_2 + t_{delay} = 54,9ms$

$t_3 = 37,1ms \rightarrow t_{delay} = g(\text{'}\underline{u1}\text{'}, Q) = \underline{19ms} \rightarrow t_{ges} = t_3 + t_{delay} = 56,1ms$

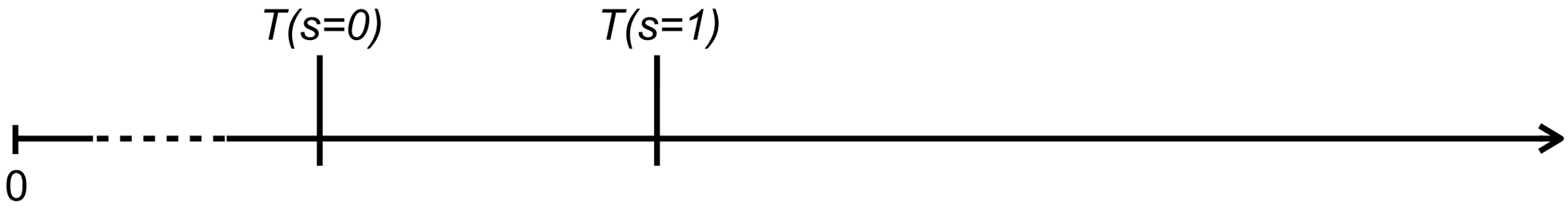
$t_4 = 36,7ms \rightarrow t_{delay} = g(\text{'}\underline{u2}\text{'}, Q) = \underline{7ms} \rightarrow t_{ges} = t_4 + t_{delay} = 43,7ms$

$t_4 = 37,6ms \rightarrow t_{delay} = g(\text{'}\underline{u2}\text{'}, Q) = \underline{7ms} \rightarrow t_{ges} = t_4 + t_{delay} = 44,6ms$

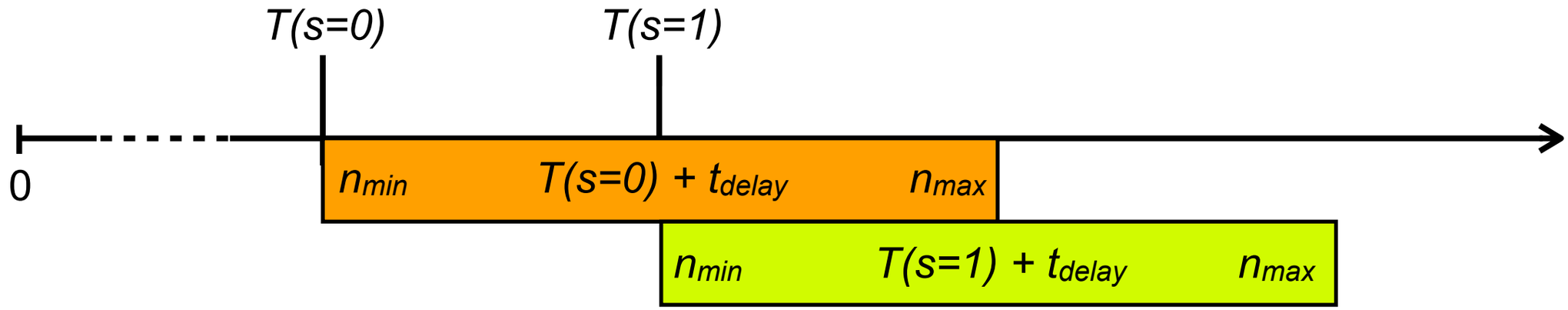
Types of Mitigation
Adding a Deterministic and Unpredictable Delay



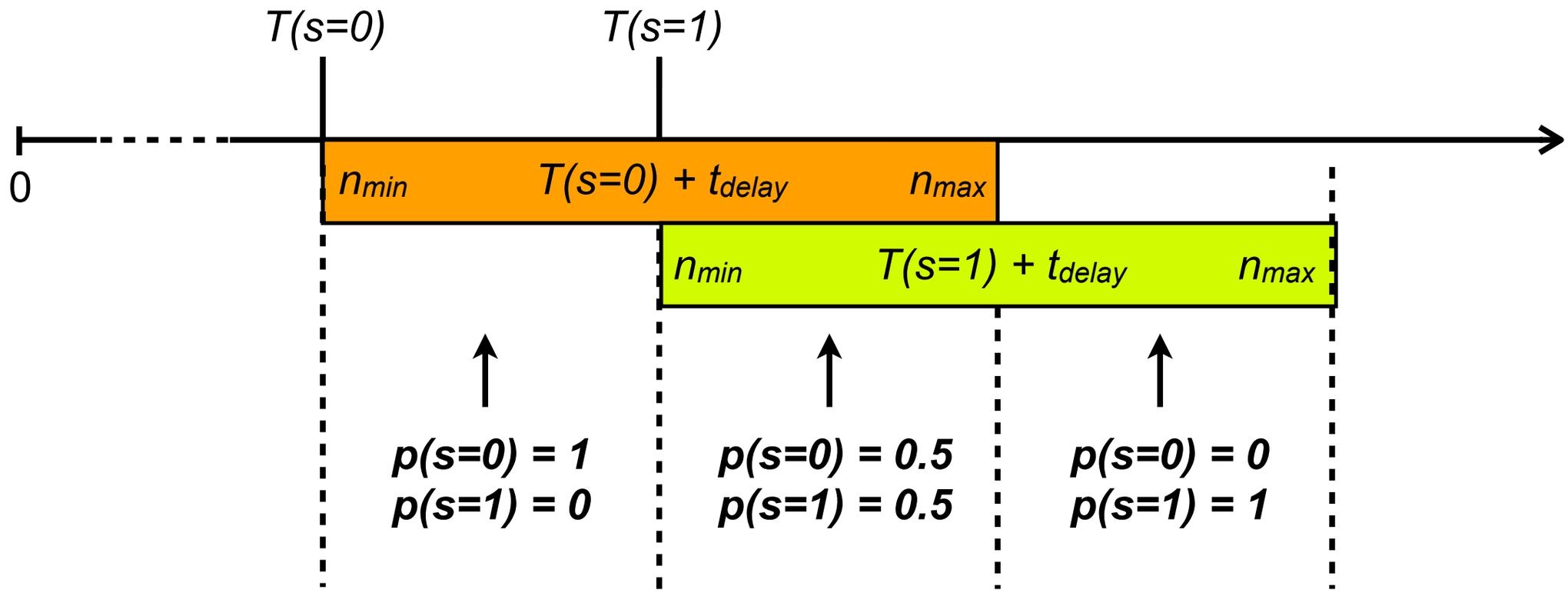
Types of Mitigation
Adding a Deterministic and Unpredictable Delay



Types of Mitigation
Adding a Deterministic and Unpredictable Delay



Types of Mitigation
Adding a Deterministic and Unpredictable Delay



Special case:
--> $T(s=1) - T(s=0) > n_{max} - n_{min}$ (No Protection)

Types of Mitigation
Adding a Deterministic and Unpredictable Delay

- Recall the necessary condition for timing side-channels to exist:

$$\forall u_a \in S, u_b \notin S : f(u_a) \neq f(u_b)$$

- The necessary condition is violated in middle area:

$$\exists u_a \in S, u_b \in S : f(u_a) \neq f(u_b)$$

Types of Mitigation
Adding a Deterministic and Unpredictable Delay

Delay type	**None**	**Pad to WCET**	**Random**	**“Fixed Random”**
Impact on Performance	Best	Worst	$t + r_{max}/2$	$t + r_{max}/2$
Impact on Security	Worst	Best	Requires more probes to cancel out noise	Offers best protection for fraction of t(s) (adjustable via r_{max})

Types of Mitigation
Adding a Deterministic and Unpredictable Delay

Delay type	None	Pad to WCET	Random	"Fixed Random"
Impact on Performance	Best	Worst	$t + r_{max}/2$	$t + r_{max}/2$
Impact on Security	Worst	Best	Requires more probes to cancel out noise	Offers best protection for fraction of t(s) (adjustable via r_{max})

Friedrich-Alexander-Universität Erlangen-Nürnberg

USIFES

Types of Mitigation
Adding a Deterministic and Unpredictable Delay

Delay type	**None**	**Pad to WCET**	**Random**	**“Fixed Random”**
Impact on Performance	Best	Worst	$t + r_{max}/2$	$t + r_{max}/2$
Impact on Security	Worst	Best	Requires more probes to cancel out noise	Offers best protection for fraction of t(s) (adjustable via r_{max})

Types of Mitigation
Adding a Deterministic and Unpredictable Delay

Delay type	**None**	**Pad to WCET**	**Random**	**“Fixed Random”**
Impact on Performance	Best	Worst	$t + r_{max}/2$	$t + r_{max}/2$
Impact on Security	Worst	Best	Requires more probes to cancel out noise	Offers best protection for fraction of t(s) (adjustable via r_{max})

Types of Mitigation
Adding a Deterministic and Unpredictable Delay

Delay type	None	Pad to WCET	Random	"Fixed Random"
Impact on Performance	Best	Worst	$t + r_{max}/2$	$t + r_{max}/2$
Impact on Security	Worst	Best	Requires more probes to cancel out noise	Offers best protection for fraction of t(s) (adjustable via r_{max})

Friedrich-Alexander-Universität Erlangen-Nürnberg

USIFES

Ongoing research

- Implement DUDe in real live applications vulnerable of timing leaks
- Empirically compare random delays and DUDe

Friedrich-Alexander-Universität Erlangen-Nürnberg

USIFES

Thanks for your attention!

Discussion...

Friedrich-Alexander-Universität Erlangen-Nürnberg

USIFES