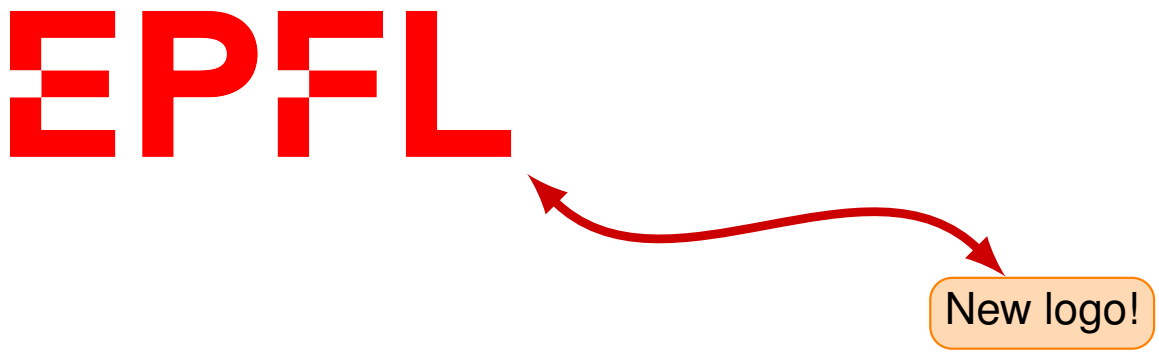
The Ratchet Race

Andrea Caforio, F Betül Durak, Serge Vaudenay



Several Competing Protocols

PR: **Poettering, Rösler**, CRYPTO 2018

JS: **Jaeger, Stepanovs**, CRYPTO 2018

BARK: our protocol, Eprint 2018/889

ACD: **Alwen, Coretti, Dodis**, this conference

JMM: **Jost, Maurer, Mularczyk**, this conference

new: our new protocol!

Several Competing Protocols

PR: **Poettering, Rösler**, CRYPTO 2018

JS: **Jaeger, Stepanovs**, CRYPTO 2018

BARK: our protocol, Eprint 2018/889

ACD: **Alwen, Coretti, Dodis**, this conference

JMM: **Jost, Maurer, Mularczyk**, this conference

new: our new protocol!

Several Competing Protocols

PR: **Poettering, Rösler**, CRYPTO 2018

JS: **Jaeger, Stepanovs**, CRYPTO 2018

BARK: our protocol, Eprint 2018/889

ACD: **Alwen, Coretti, Dodis**, this conference

JMM: **Jost, Maurer, Mularczyk**, this conference

new: our new protocol!

Several Competing Protocols

PR: **Poettering, Rösler**, CRYPTO 2018

JS: **Jaeger, Stepanovs**, CRYPTO 2018

BARK: our protocol, Eprint 2018/889

ACD: **Alwen, Coretti, Dodis**, this conference

JMM: **Jost, Maurer, Mularczyk**, this conference

new: our new protocol!

Which Comparison Metrics?

- **security**
  - forward secrecy
  - postcompromise security
  - time to heal
  - bad randomness resilience
  - unforgeability
  - DoS resilience
- **efficiency**
  - runtime
  - message size
  - state size
- **incident awareness**
  - forgery detection
  - explicit ACK
- **functionality**
  - multi-device
  - immediate decryption?
  - on-demand ratchet?

Which Comparison Metrics?

- **security**
  - forward secrecy
  - postcompromise security
  - time to heal
  - bad randomness resilience
  - unforgeability
  - DoS resilience
- **efficiency**
  - runtime
  - message size
  - state size
- **incident awareness**
  - forgery detection
  - explicit ACK
- **functionality**
  - multi-device
  - immediate decryption?
  - on-demand ratchet?

Which Comparison Metrics?

- **security**
  - forward secrecy
  - postcompromise security
  - time to heal
  - bad randomness resilience
  - unforgeability
  - DoS resilience
- **efficiency**
  - runtime
  - message size
  - state size
- **incident awareness**
  - forgery detection
  - explicit ACK
- **functionality**
  - multi-device
  - immediate decryption?
  - on-demand ratchet?

Which Comparison Metrics?

- **security**
  - forward secrecy
  - postcompromise security
  - time to heal
  - bad randomness resilience
  - unforgeability
  - DoS resilience
- **efficiency**
  - runtime
  - message size
  - state size
- **incident awareness**
  - forgery detection
  - explicit ACK
- **functionality**
  - multi-device
  - immediate decryption?
  - on-demand ratchet?

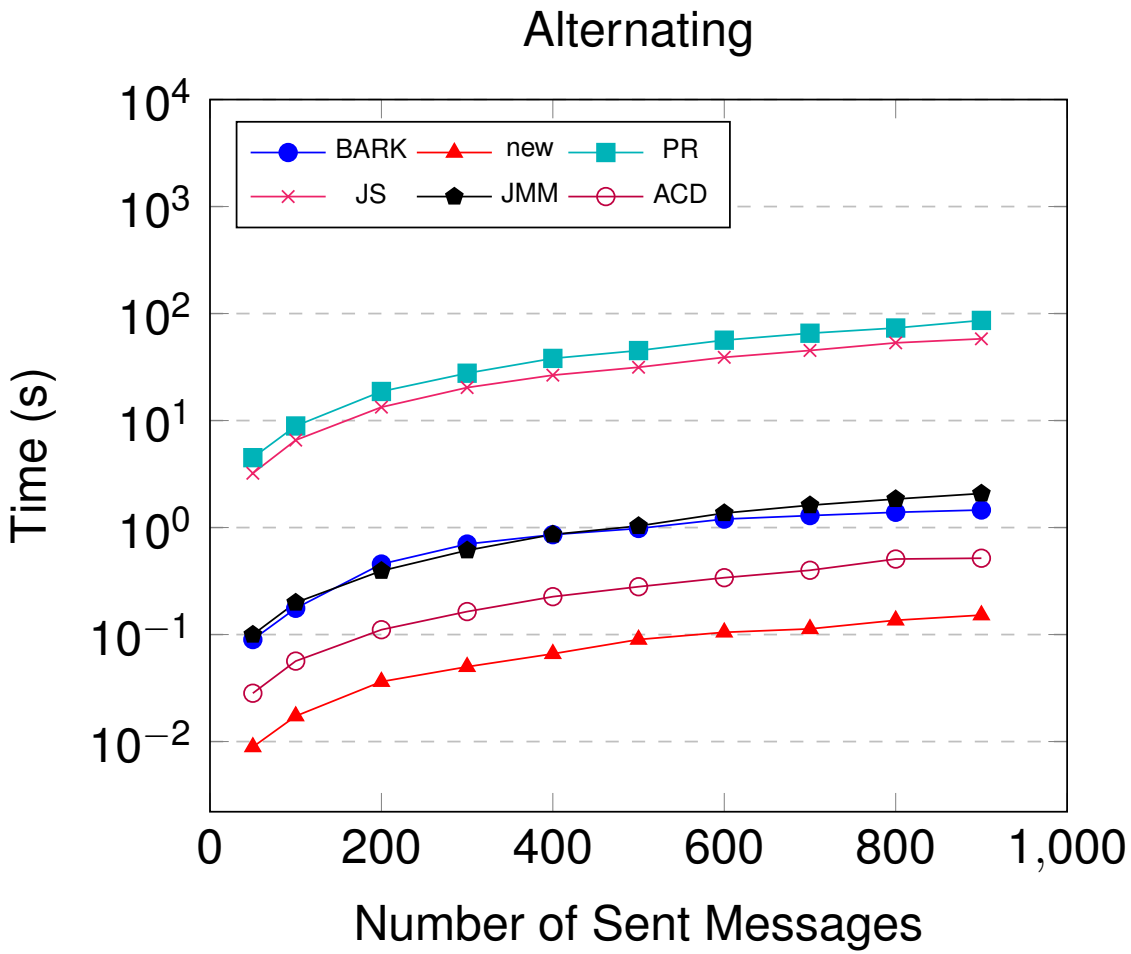
Our New Protocol

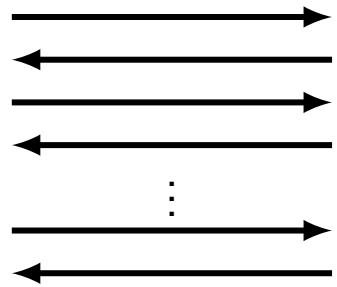
- generic composition of two protocols
- typically:

  ratchet protocol + symmetric-crypto protocol

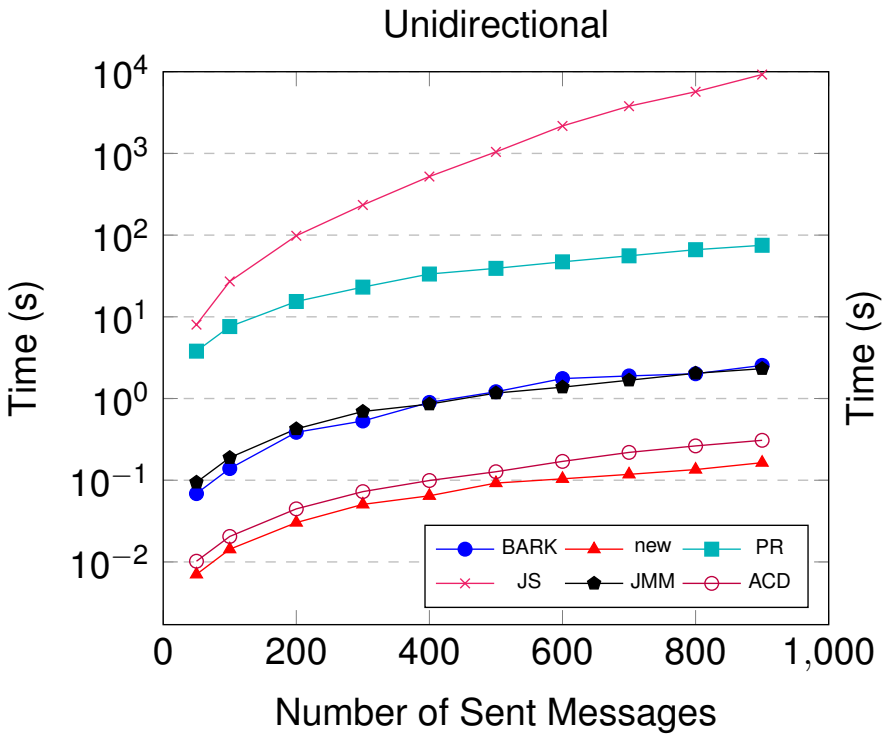
  (we don't want to ratchet too often)
- $\approx$ "double ratchet" (ACD/Signal)
  - ACD ratchets when the direction of communication changes
  - our protocol ratchets at any message **"on demand"**

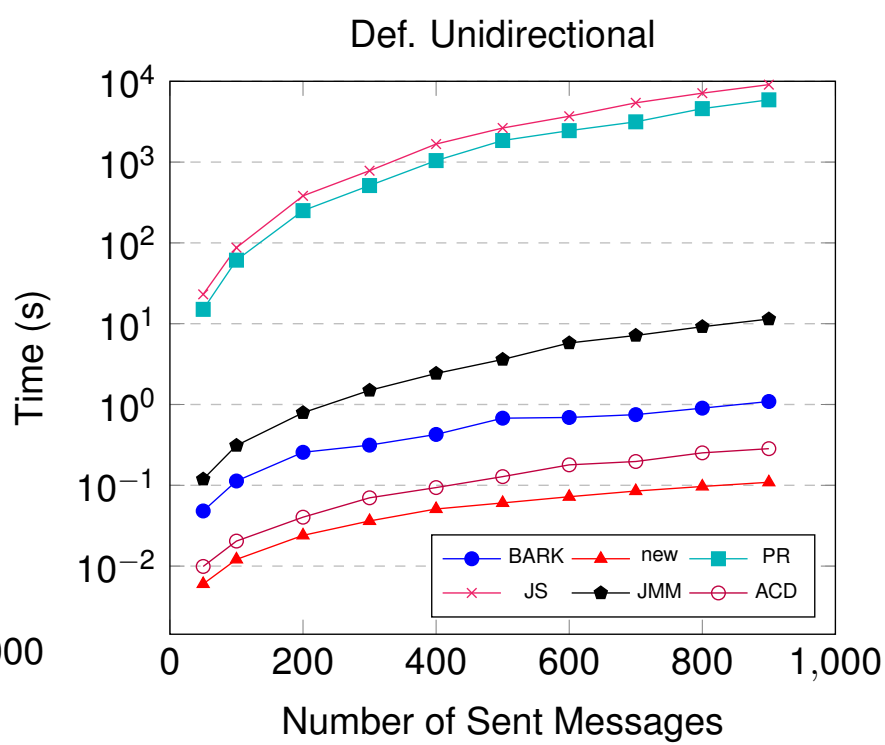
Performance (Runtime)

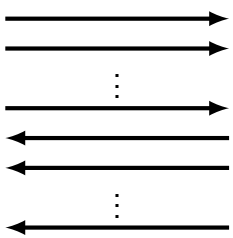


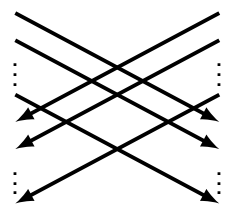


Performance (Runtime)









Comparison

* adapted to the functionality offered by the protocol

	PR	JS	BARK	JMM	ACD	new
Security	optimal	optimal	near-optimal	near-optimal	adapted*	adapted*

Comparison

* adapted to the functionality offered by the protocol

	PR	JS	BARK	JMM	ACD	new
Security	optimal	optimal	near-optimal	near-optimal	adapted*	adapted*
Complexity	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	$\mathcal{O}(n)$

Comparison

* adapted to the functionality offered by the protocol

	PR	JS	BARK	JMM	ACD	new
Security	optimal	optimal	near-optimal	near-optimal	adapted*	adapted*
Complexity	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	$\mathcal{O}(n)$
Bad \$ resilience	$-$	$+$	$-$	$+$	$+$	$-$

Comparison

* adapted to the functionality offered by the protocol

	PR	JS	BARK	JMM	ACD	new
Security	optimal	optimal	near-optimal	near-optimal	adapted*	adapted*
Complexity	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	$\mathcal{O}(n)$
Bad \$ resilience	$-$	$+$	$-$	$+$	$+$	$-$
Forgery detection	$-$	$+$	$+/-$	$-$	$-$	$+$

Comparison

* adapted to the functionality offered by the protocol

	PR	JS	BARK	JMM	ACD	new
Security	optimal	optimal	near-optimal	near-optimal	adapted*	adapted*
Complexity	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	$\mathcal{O}(n)$
Bad \$ resilience	$-$	$+$	$-$	$+$	$+$	$-$
Forgery detection	$-$	$+$	$+/-$	$-$	$-$	$+$
Explicit ACK	$+$	$+$	$+$	$+$	$-$	$+$

to be continued...

References

- BARK: Eprint 2018/889
- new protocol: on eprint soon
- implementations:

  `https://github.com/qantik/ratcheted`