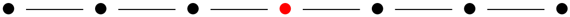
Multiple Forking: Deconstructed, Unified

Sanjit Chatterjee and Chethan Kamath

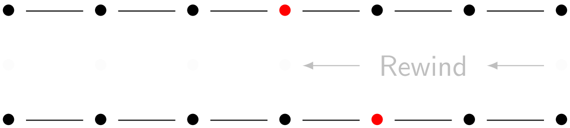
Indian Institute of Science, Bangalore

December 3, 2013

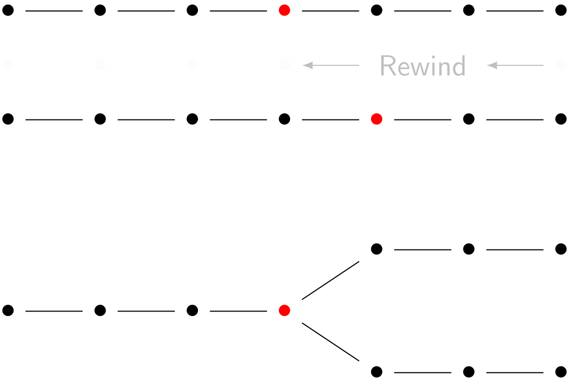
Elementary Forking (1 RO, 1 Fork)



Elementary Forking (1 RO, 1 Fork)



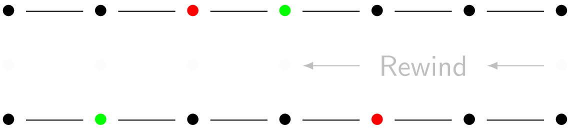
Elementary Forking (1 RO, 1 Fork)



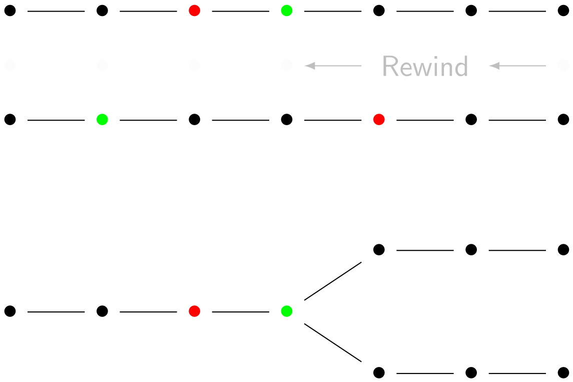
Cost: $\mathrm{O}(q)$

Multiple Forking (2 ROs, 1 Fork)

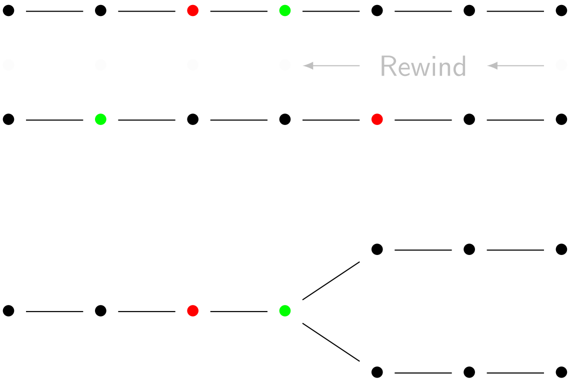
Multiple Forking (2 ROs, 1 Fork)



Multiple Forking (2 ROs, 1 Fork)

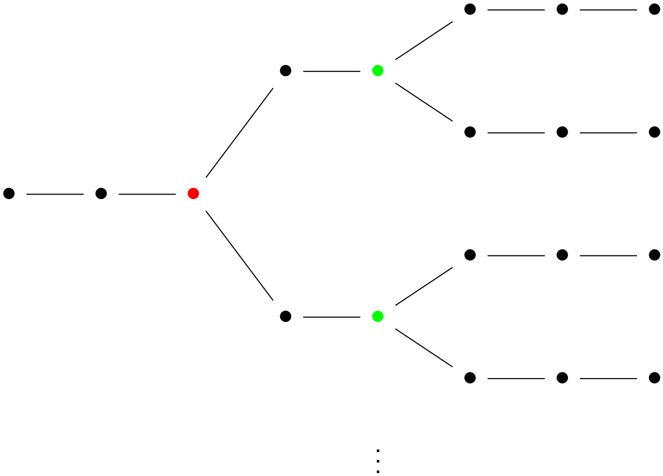


Multiple Forking (2 ROs, 1 Fork)

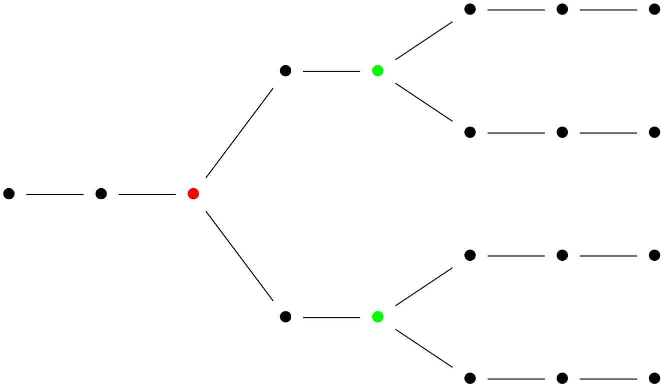


Cost: $O\left(q^2\right)$

Multiple Forking (2 ROs, *n* Forks)



Multiple Forking (2 ROs, *n* Forks)



⋮

Cost: $O\left(q^{2n}\right)$

Applications

1. Proxy Signatures [BPW12]
2. Identity-Based Signatures [GG09]
3. ZK Arguments [CMW13]

Applications

1. Proxy Signatures [BPW12]
2. Identity-Based Signatures [GG09]
3. ZK Arguments [CMW13]

Can we improve on $\mathrm{O}\left(q^{2n}\right)$?

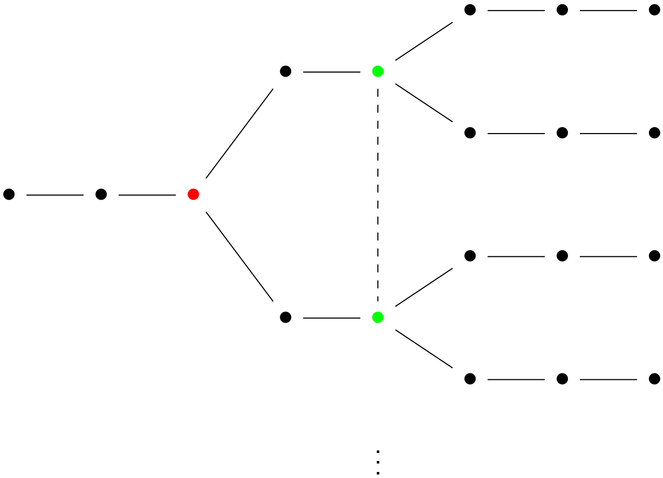
Applications

1. Proxy Signatures [BPW12]
2. Identity-Based Signatures [GG09]
3. ZK Arguments [CMW13]

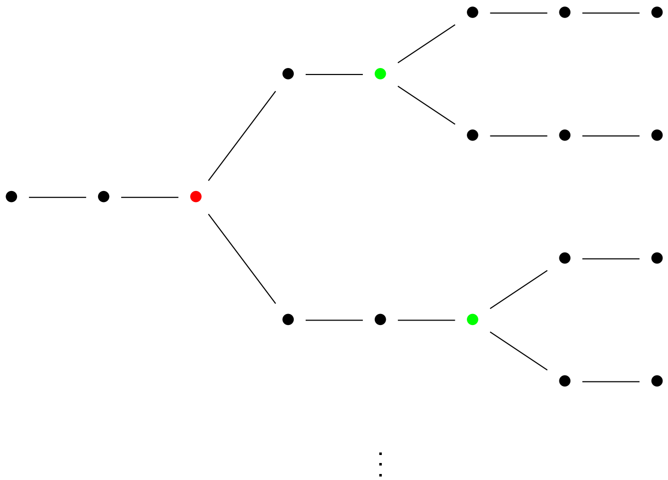
Can we improve on $\mathrm{O}\left(q^{2n}\right)$?

Reduced to $\mathrm{O}\left(q^{n}\right)$

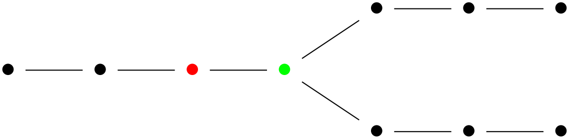
Observation 1: Index Independence



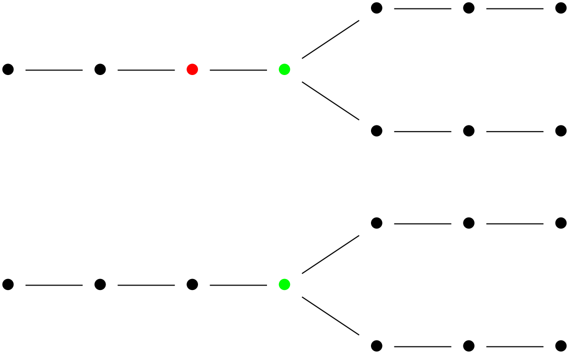
Observation 1: Index Independence



Observation 2: R-O Dependence



Observation 2: R-O Dependence



“R-O binding”

Result

Index Independence + RO Dependence

Cost *per* fork: down from $\mathrm{O}\left(q^2\right)$ to $\mathrm{O}\left(q\right)$
Total cost: down from $\mathrm{O}\left(q^{2n}\right)$ to $\mathrm{O}\left(q^n\right)$

Result

Index Independence + RO Dependence

Cost *per* fork: down from $\mathrm{O}\left(q^2\right)$ to $\mathrm{O}\left(q\right)$
Total cost: down from $\mathrm{O}\left(q^{2n}\right)$ to $\mathrm{O}\left(q^n\right)$

Optimal, can be extended to arbitrary r ROs
Unified Model for Multiple Forking

Thank you!

What did the annoyed forking algorithm tell the adversary?

Thank you!

What did the annoyed forking algorithm tell the adversary?

Fork you.

Thank you!

What did the annoyed forking algorithm tell the adversary?

Fork you.

Well, let me get my coat.