UROP - Undergraduate Research Opportunities Programme

ALPHA

Adaptive and Lightweight Protocol for Hop-by-Hop Authentication

Florian Weingarten Johannes Gilger

Lehrstuhl für Informatik IV
LuFG Verteilte Systeme

Was möchten wir heute vorstellen?

- Wofür braucht man Alpha?
- Was tut Alpha?
- Was haben wir in unserem Projekt gemacht?
- Welche Funktionen hat unsere Software?
- Welche Probleme traten auf?
- Wie könnte die Zukunft von Alpha aussehen?

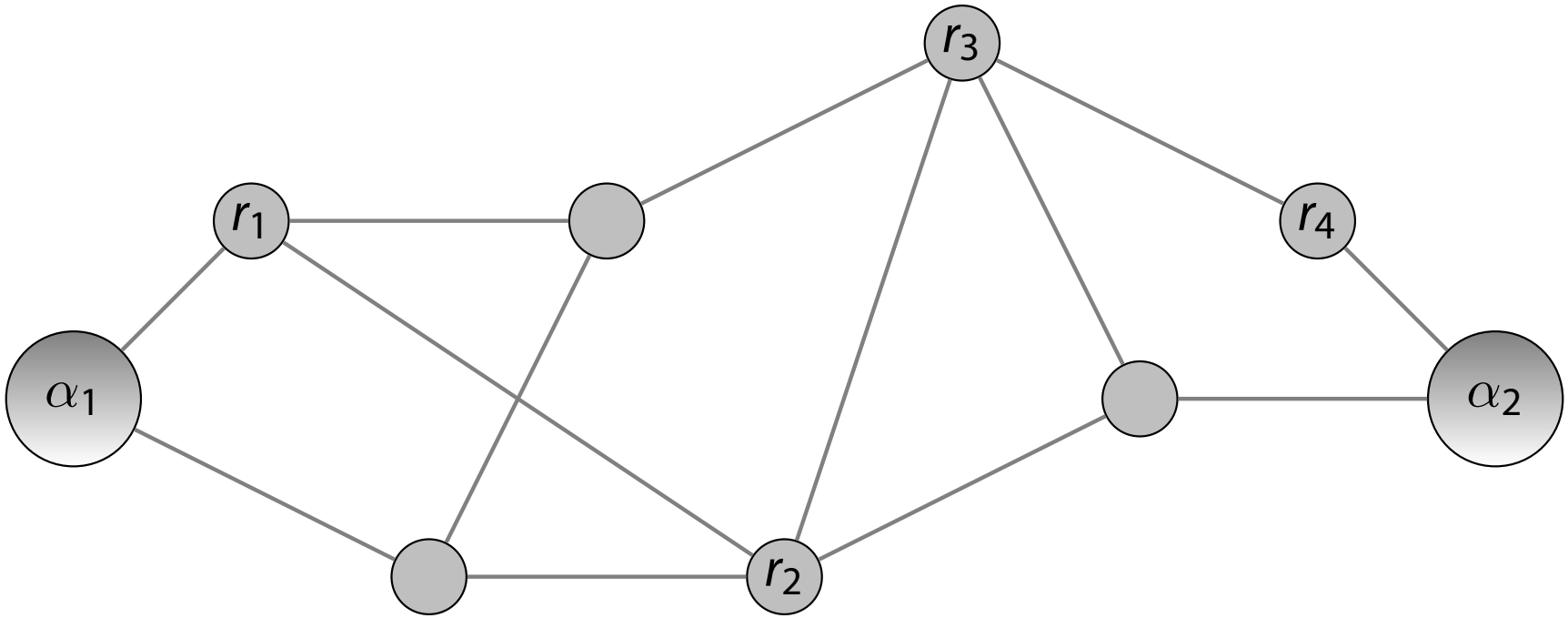
Wofür braucht man Alpha?

Alpha kann man benutzen um . . .

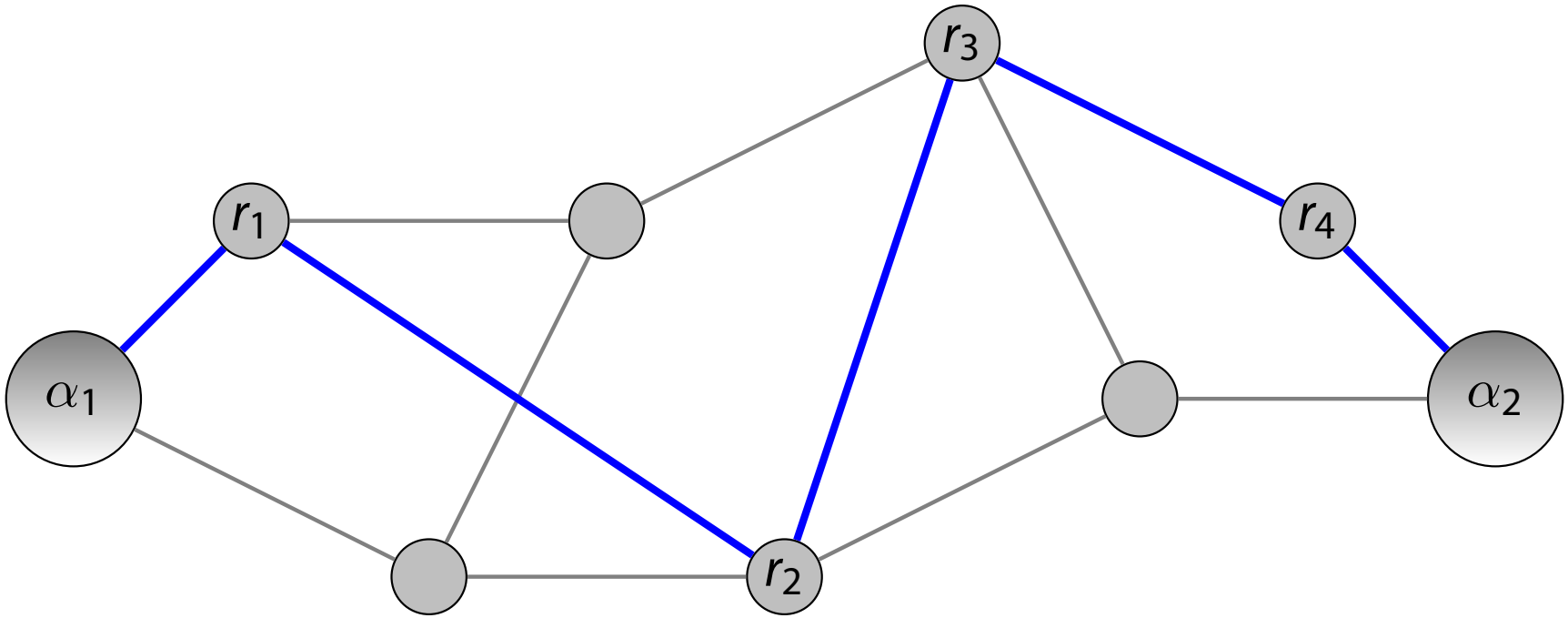
- . . . kleine Netzwerkgeräte vor unnötigem Datenverkehr zu schützen
  - Daten, die manipuliert wurden
  - Daten mit gefälschtem Absender
  - Daten, die die Resourcen des Geräts aufbrauchen
- . . . Stabilität und Durchsatz des gesamten Netzwerks zu verbessern

Was tut Alpha?

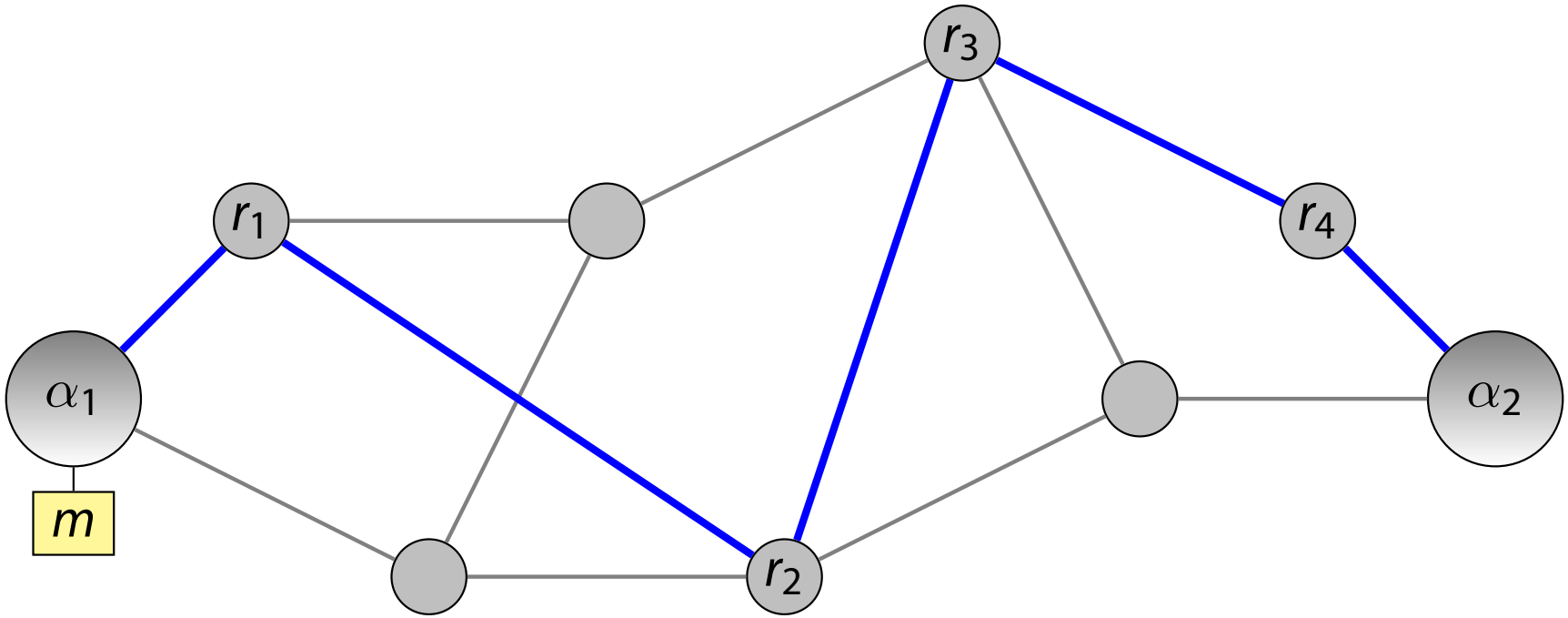
Was tut Alpha?



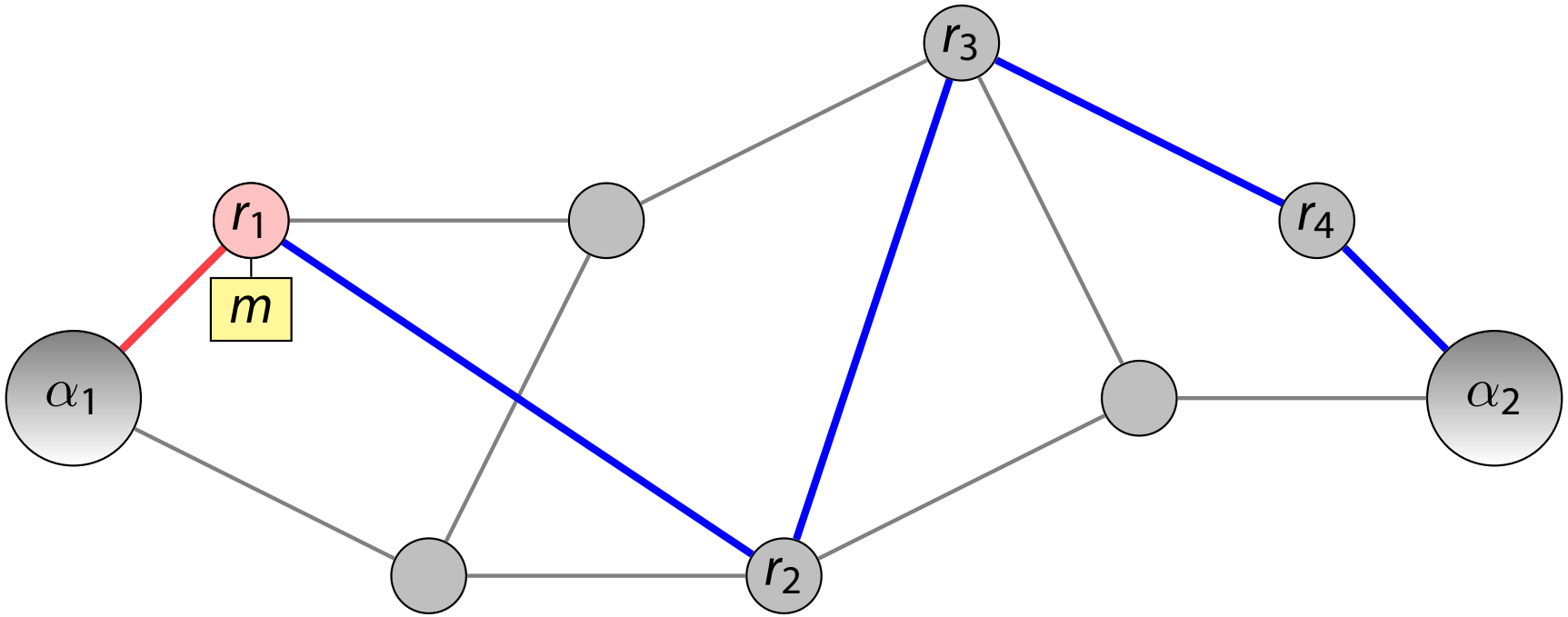
Was tut Alpha?



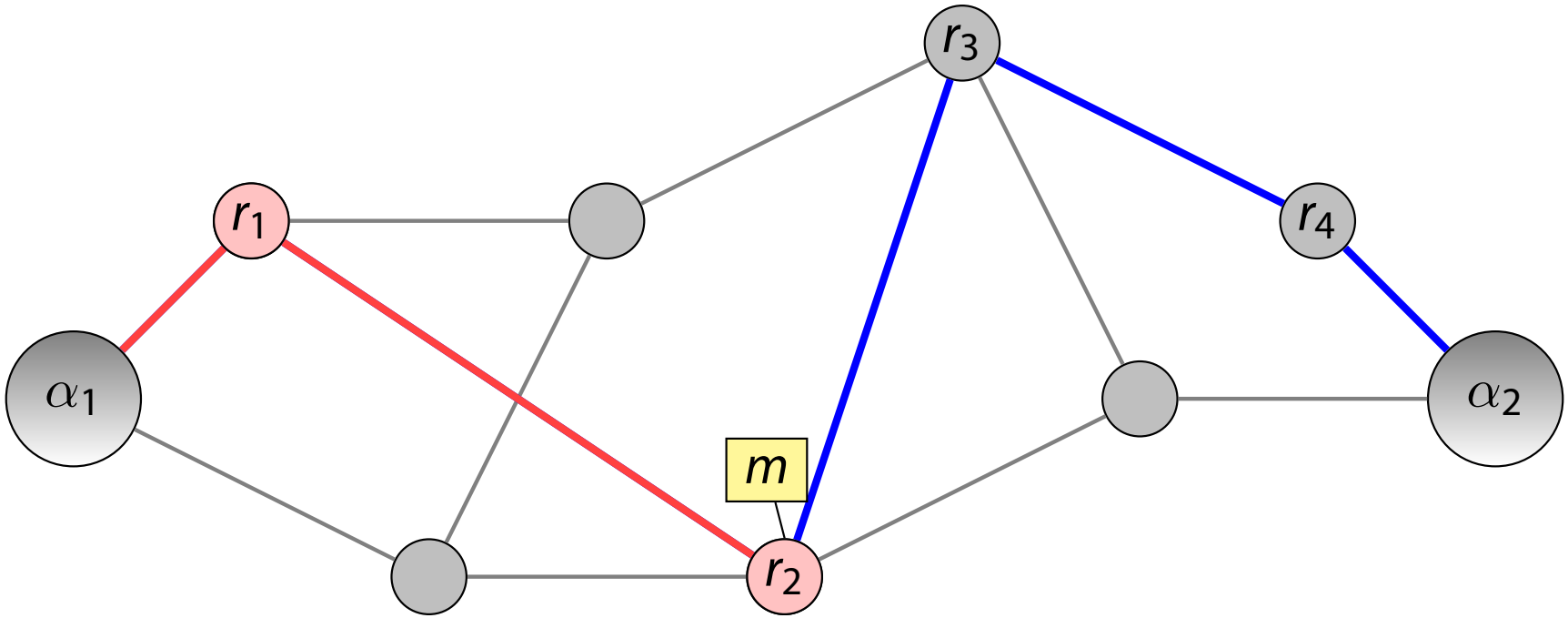
Was tut Alpha?



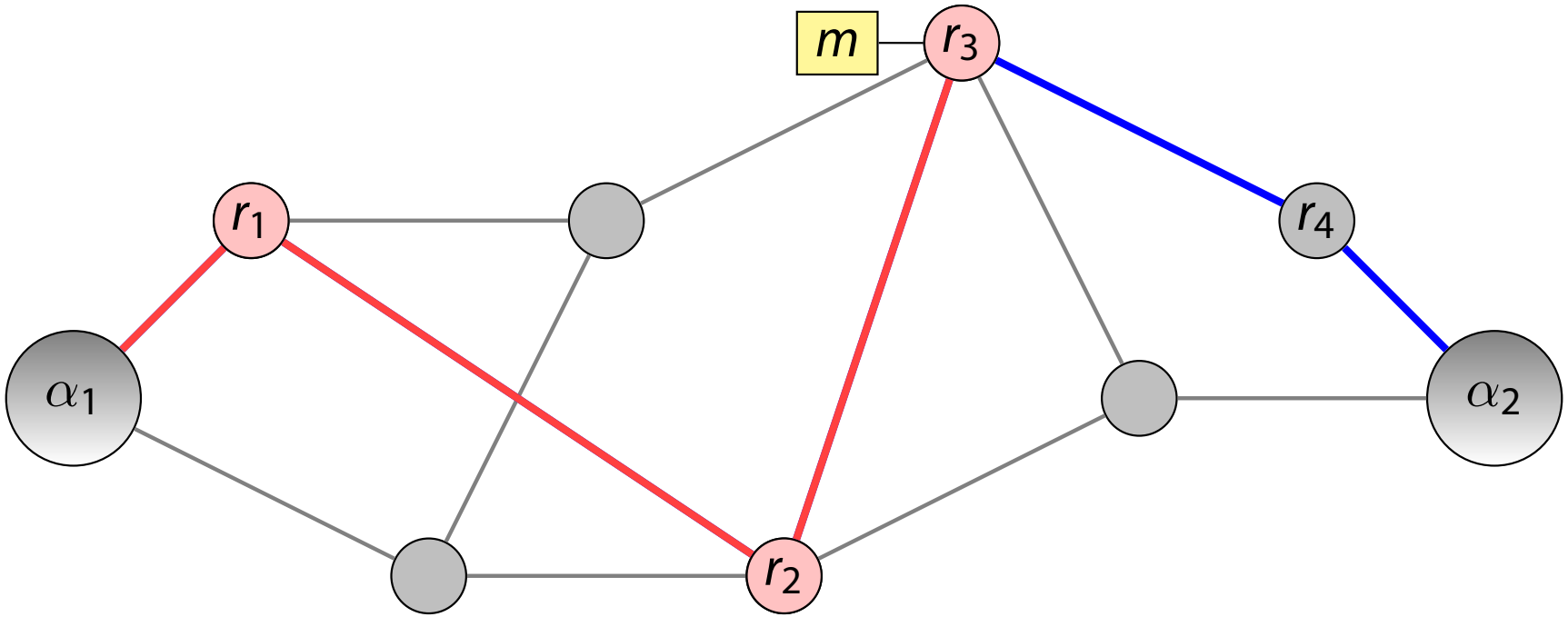
Was tut Alpha?



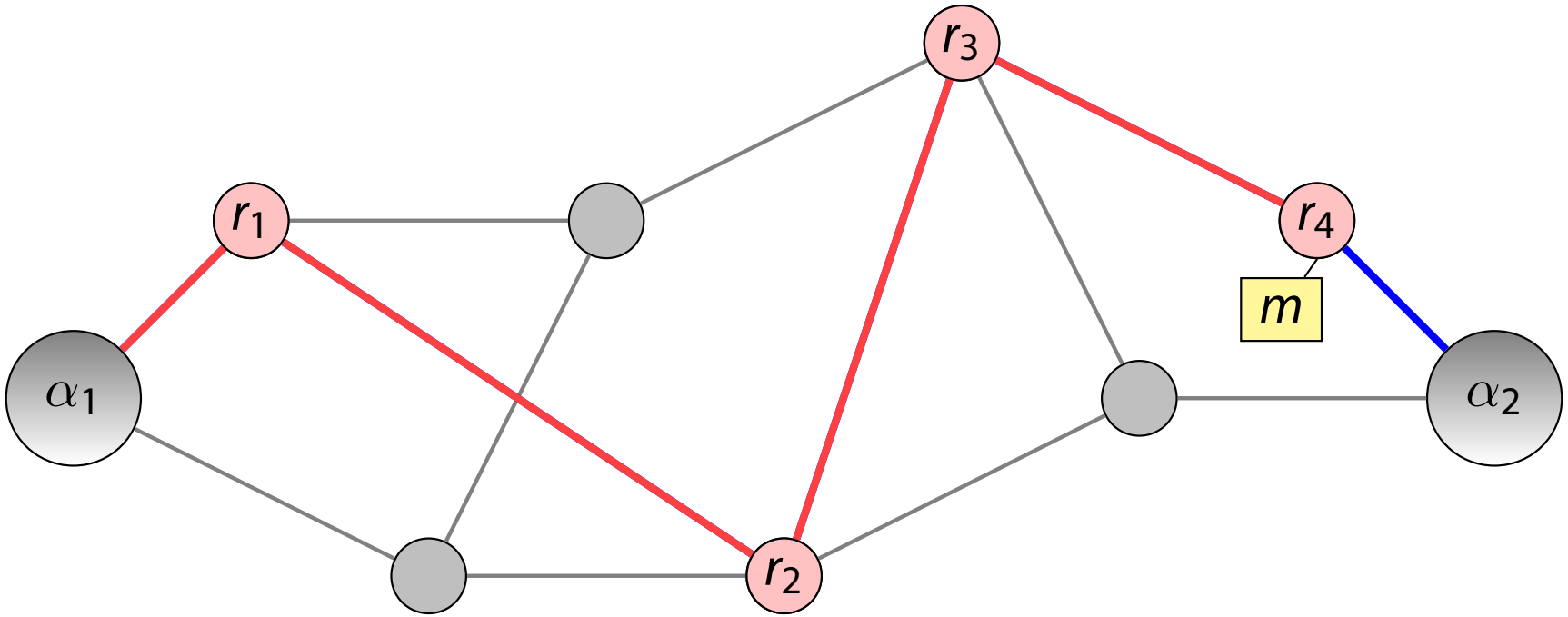
Was tut Alpha?



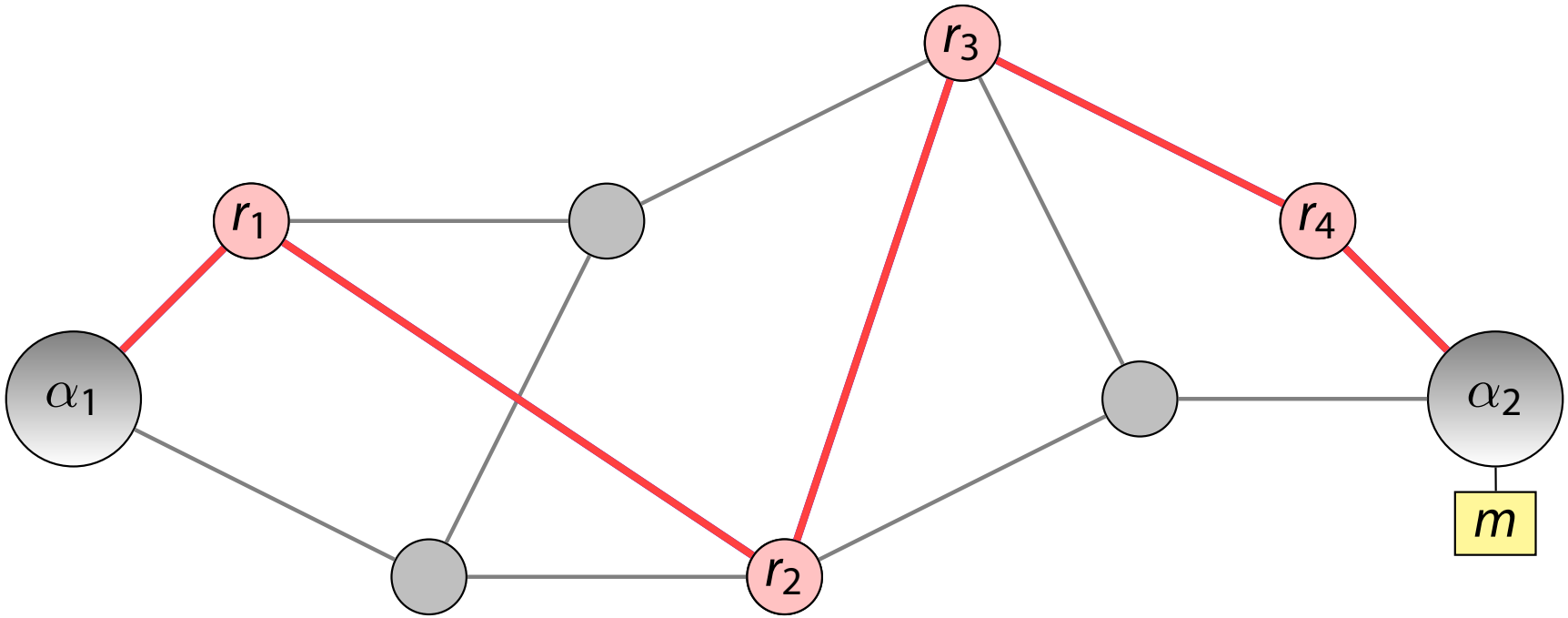
Was tut Alpha?



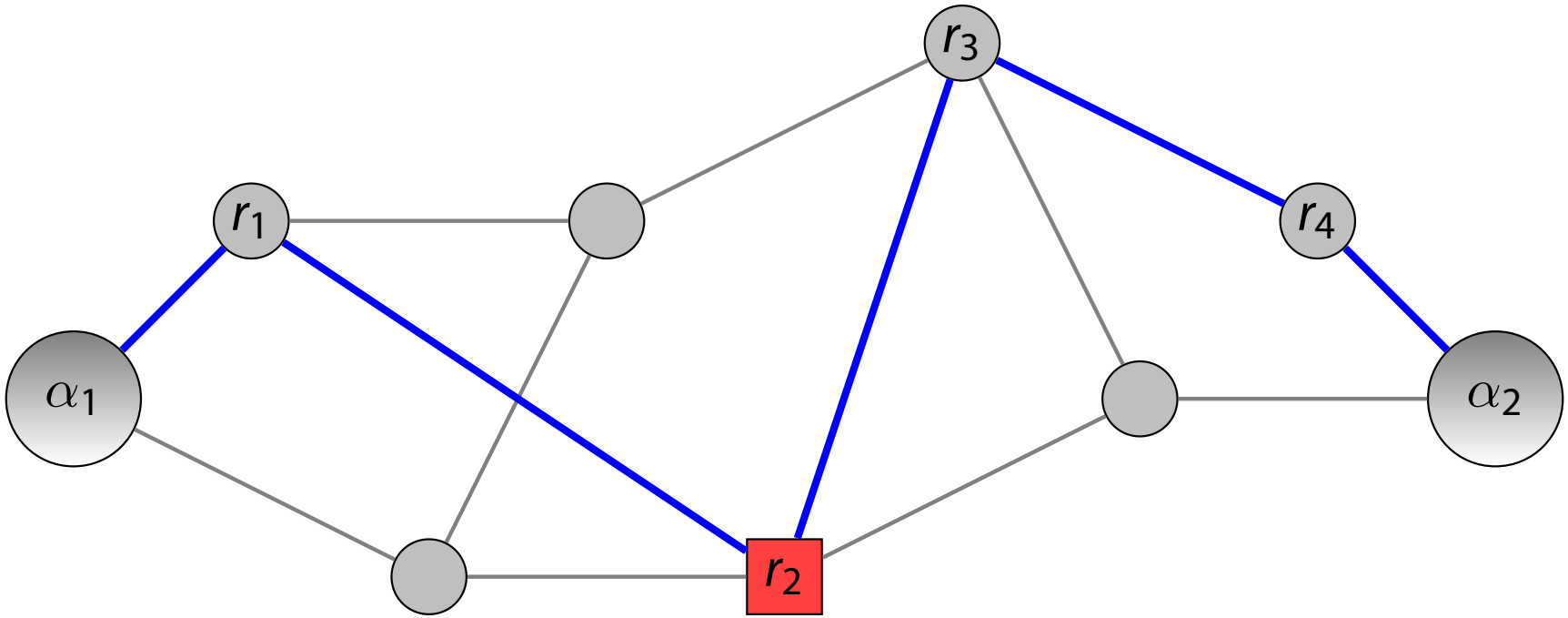
Was tut Alpha?



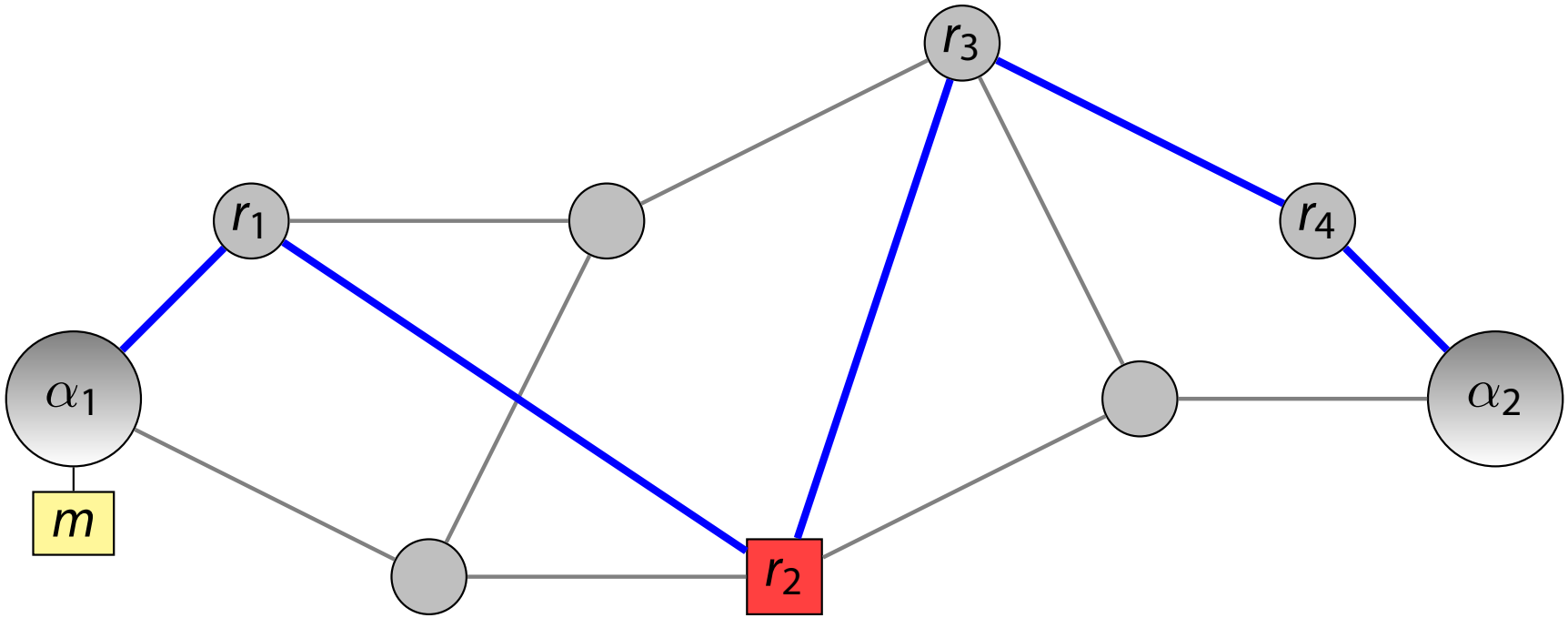
Was tut Alpha?



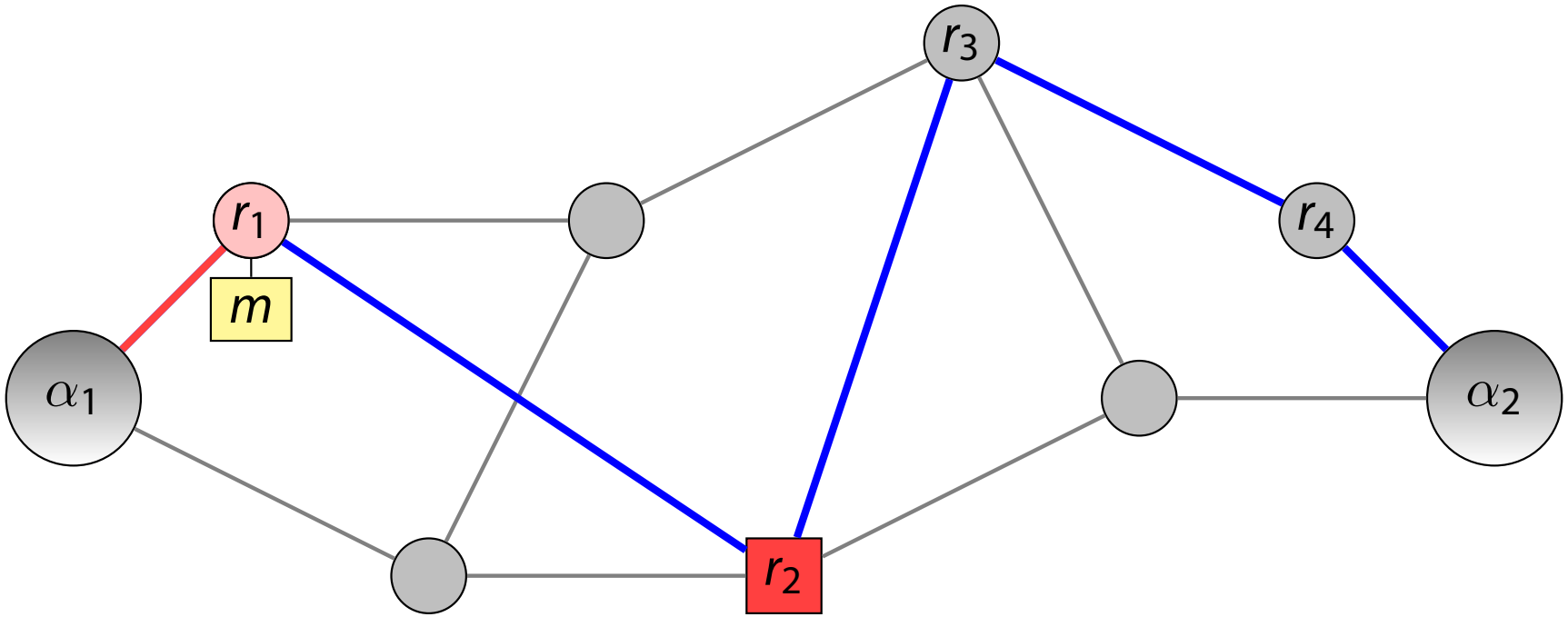
Was tut Alpha?



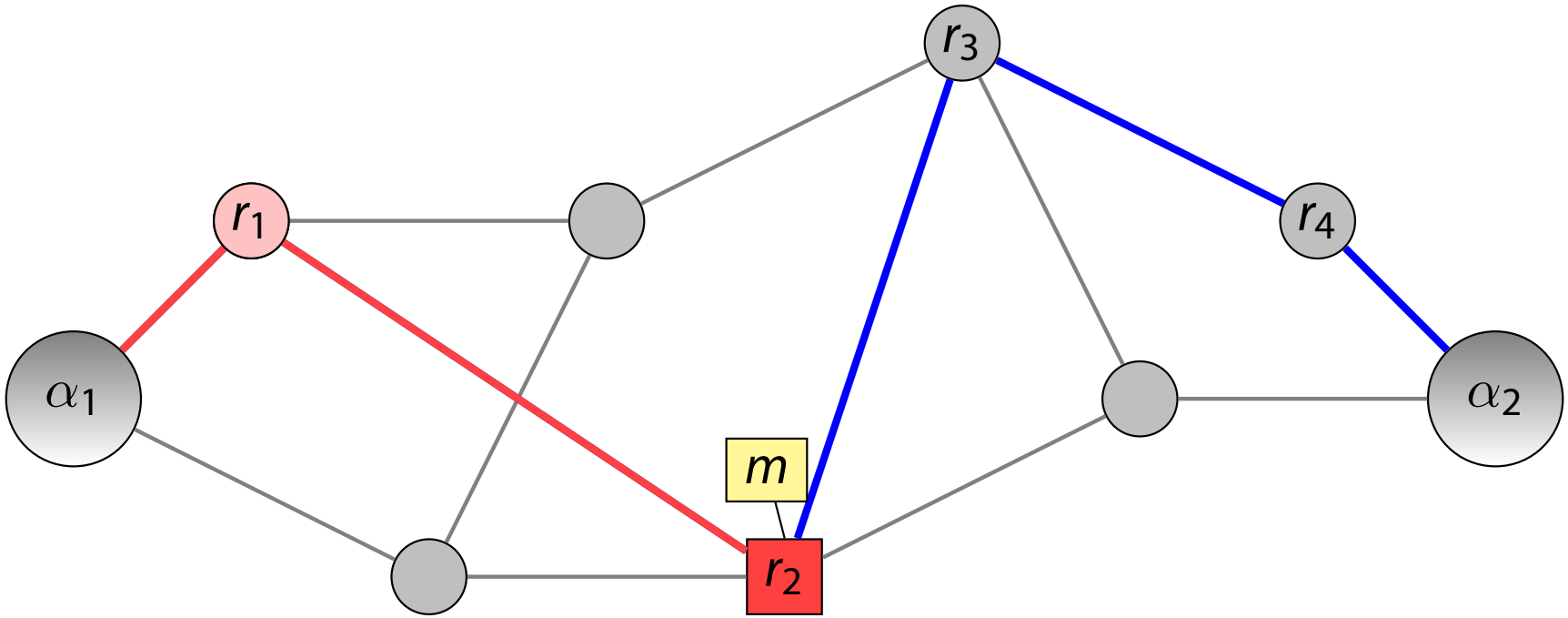
Was tut Alpha?



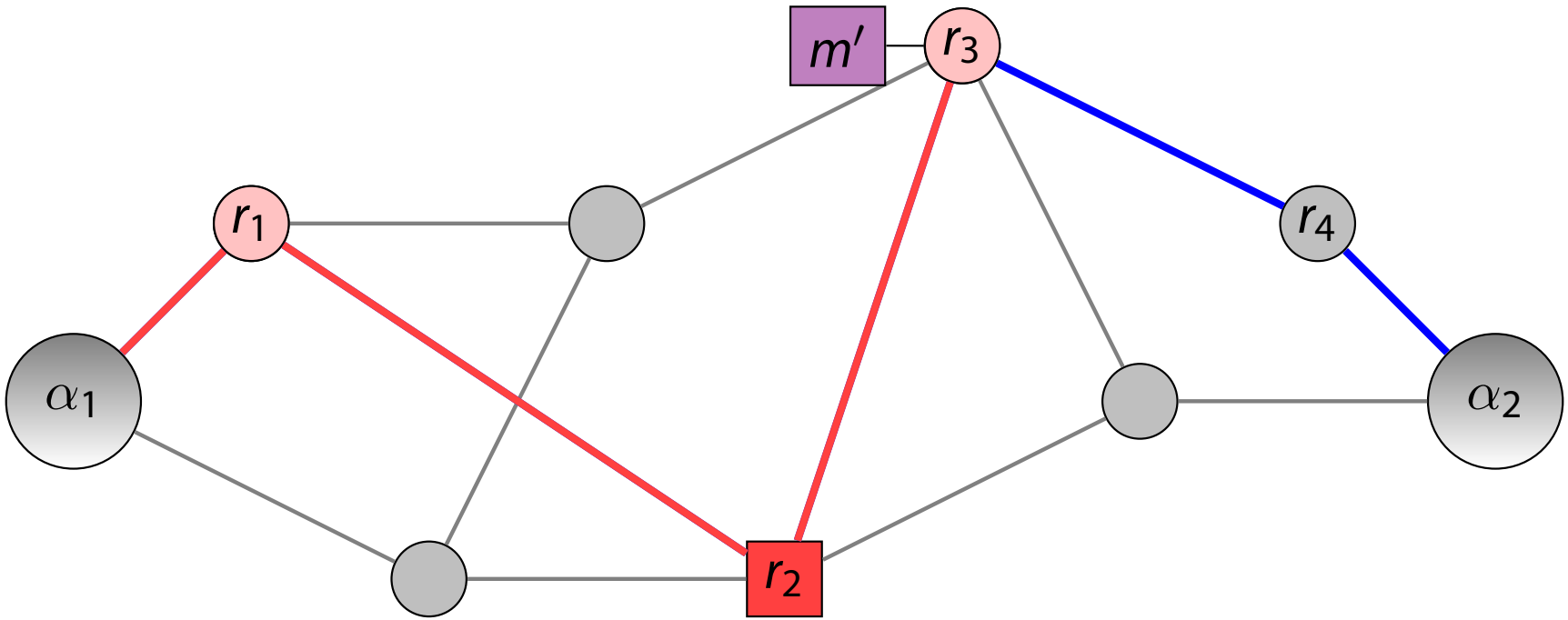
Was tut Alpha?



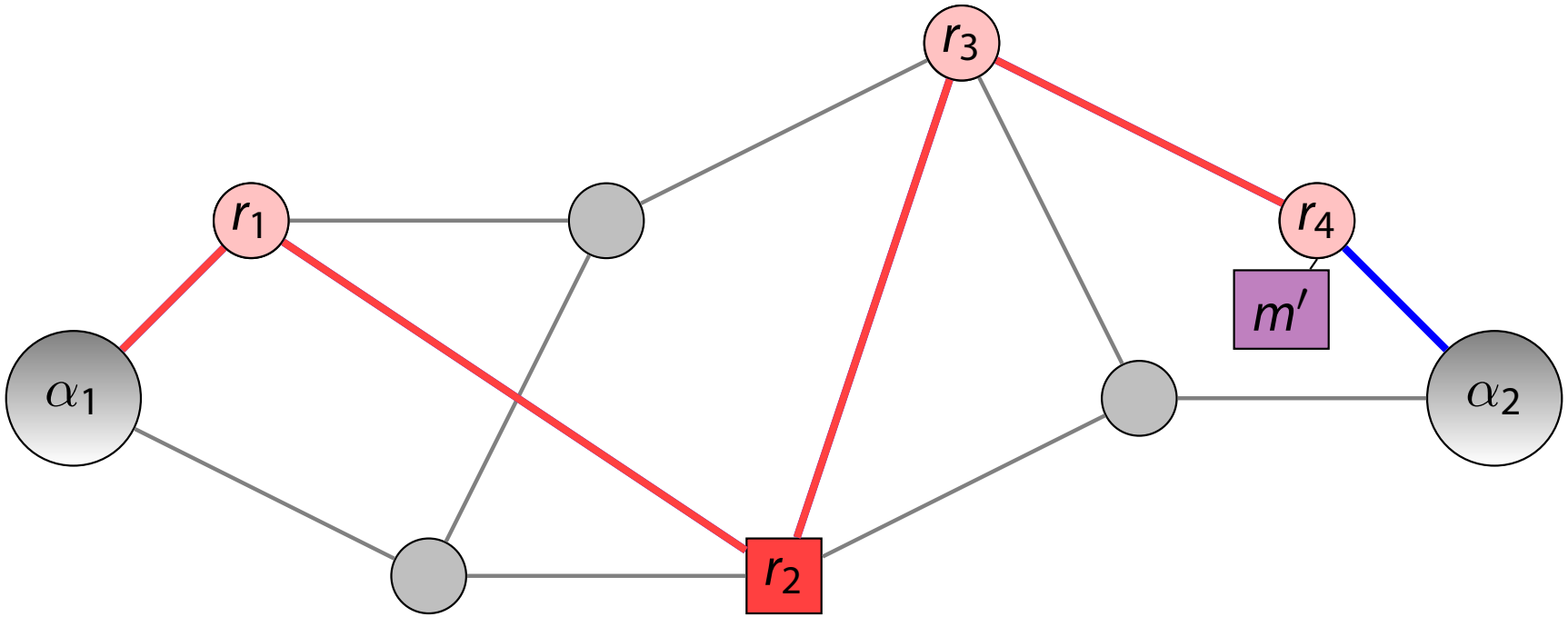
Was tut Alpha?



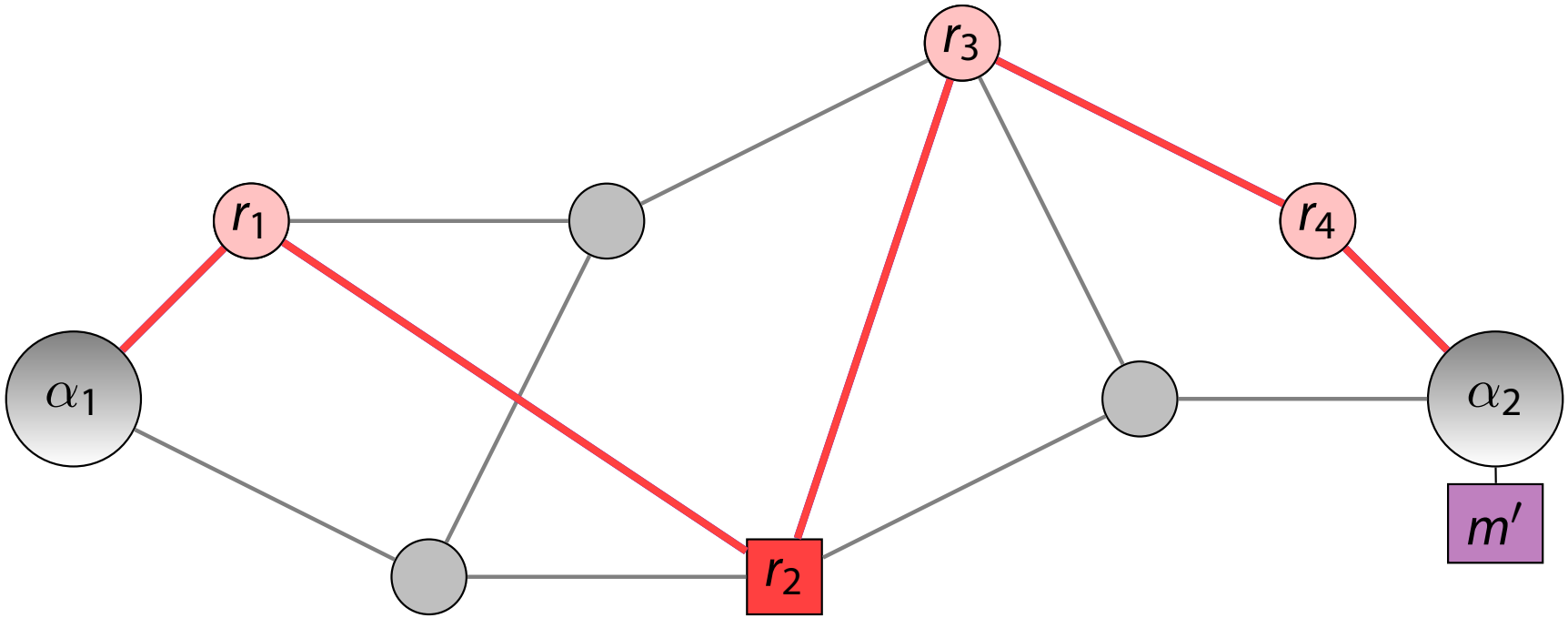
Was tut Alpha?



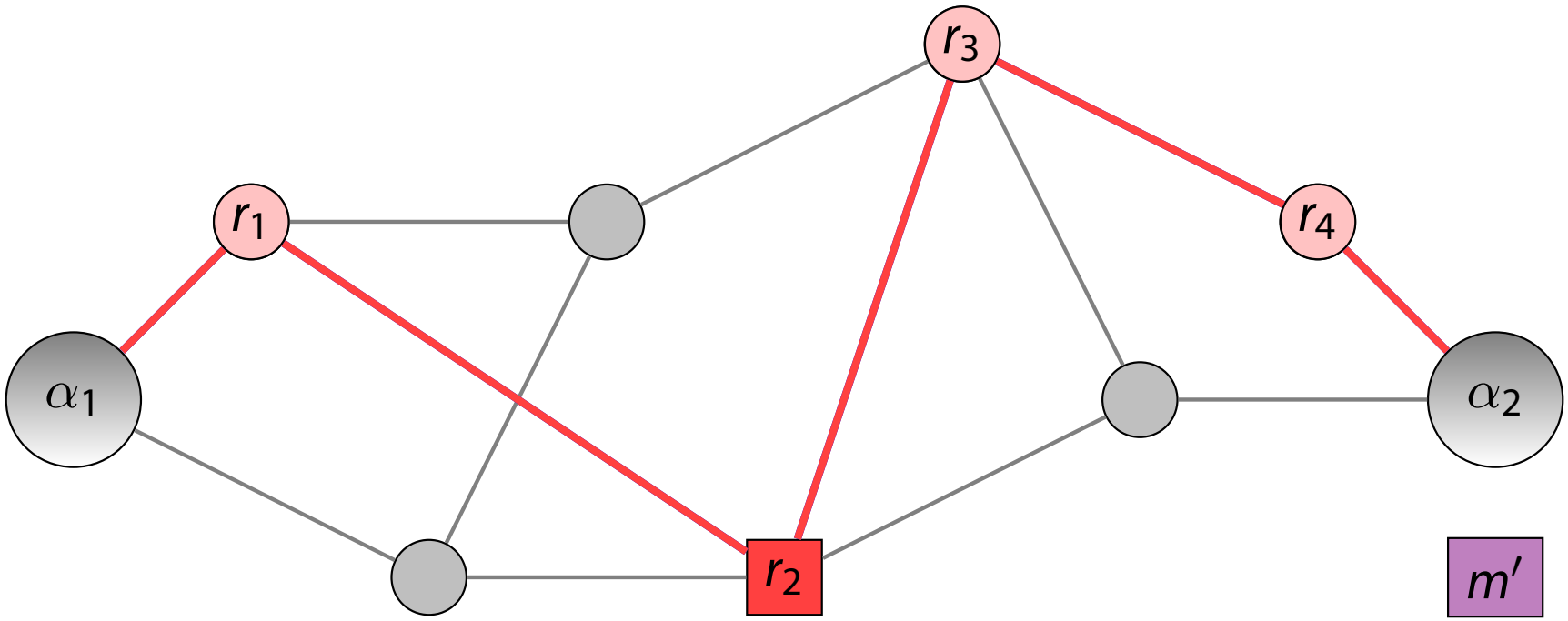
Was tut Alpha?



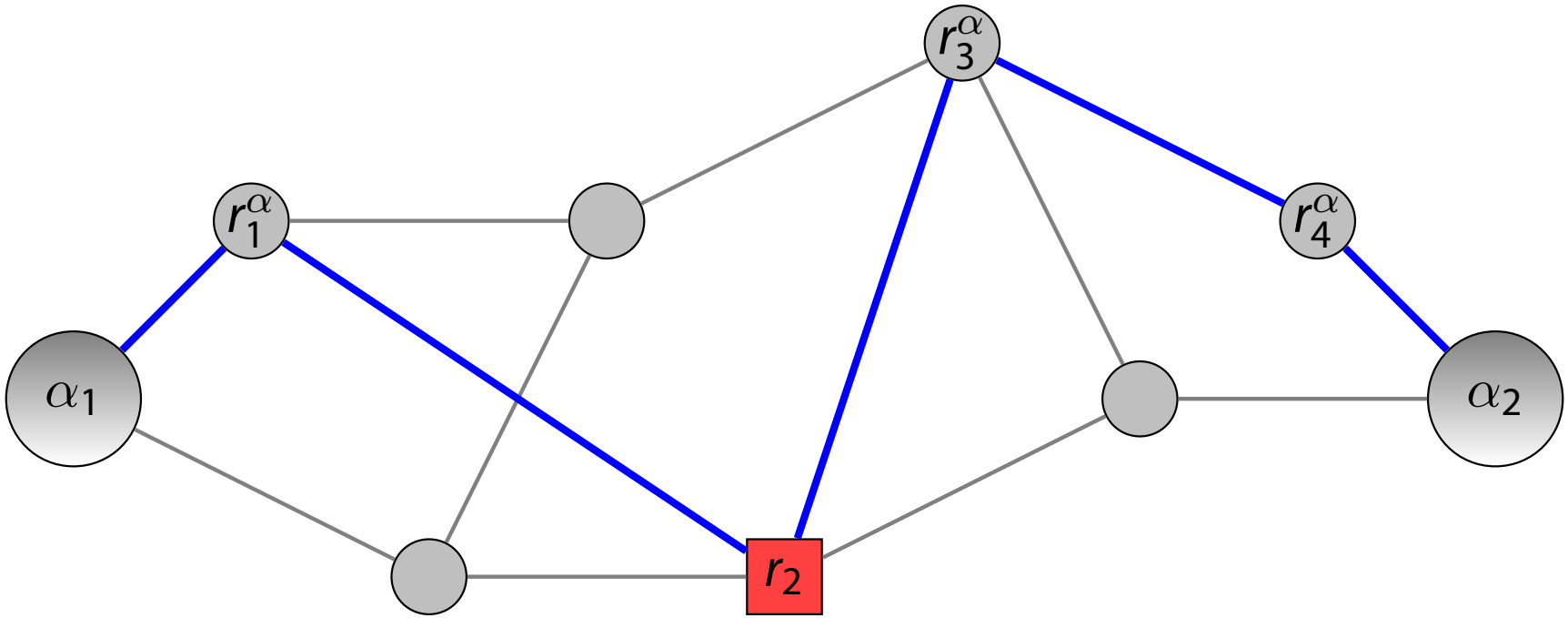
Was tut Alpha?



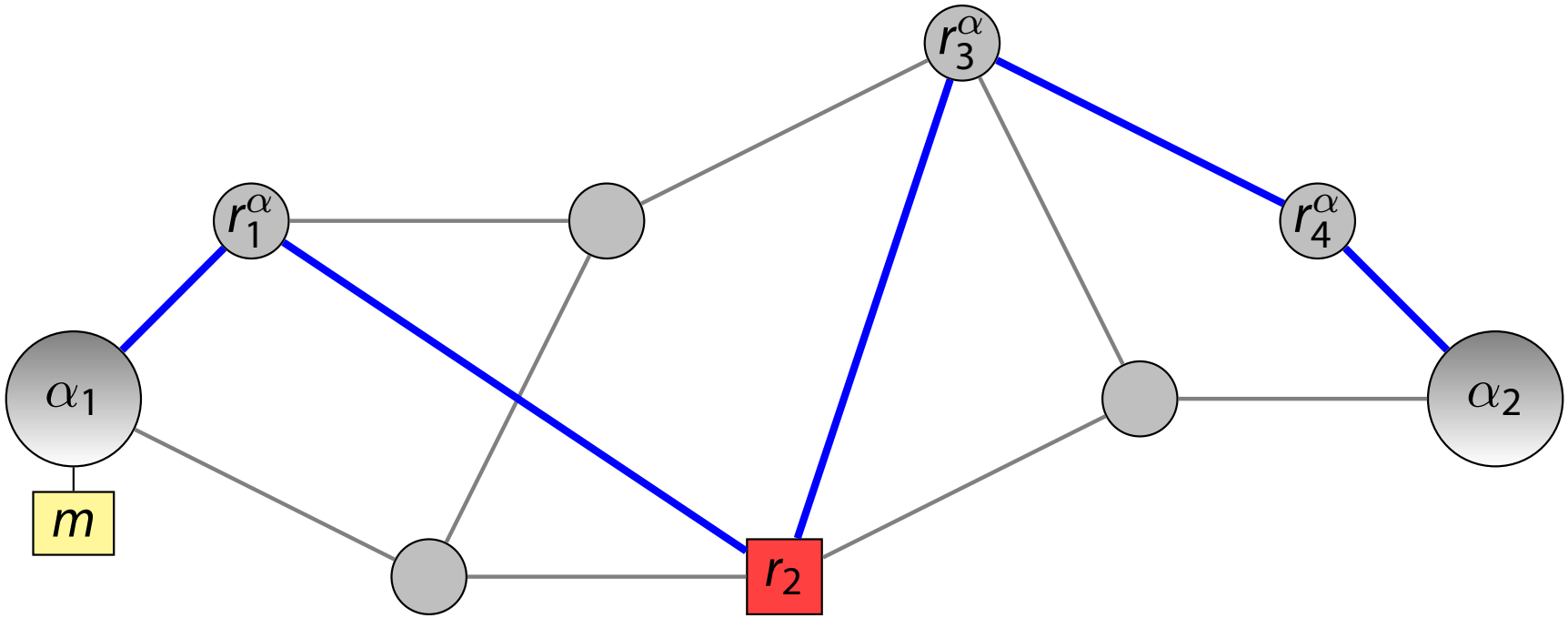
Was tut Alpha?



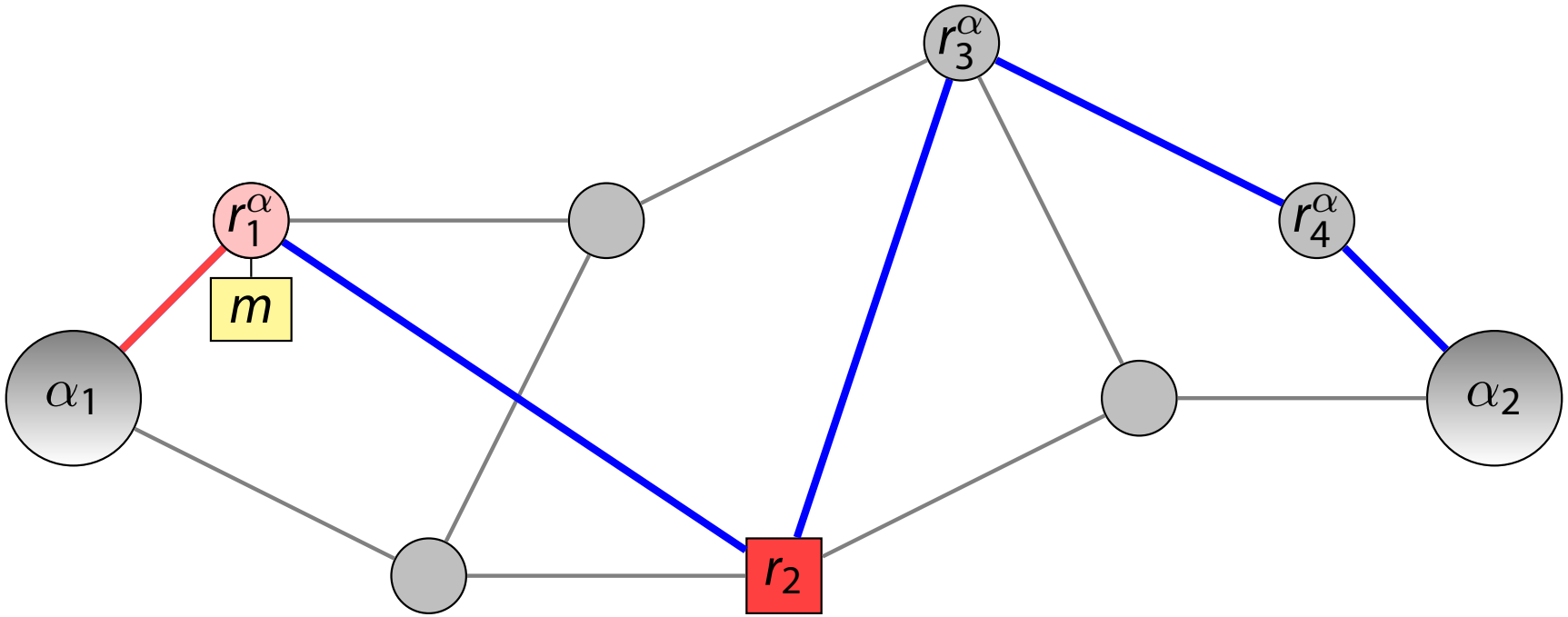
Was tut Alpha?



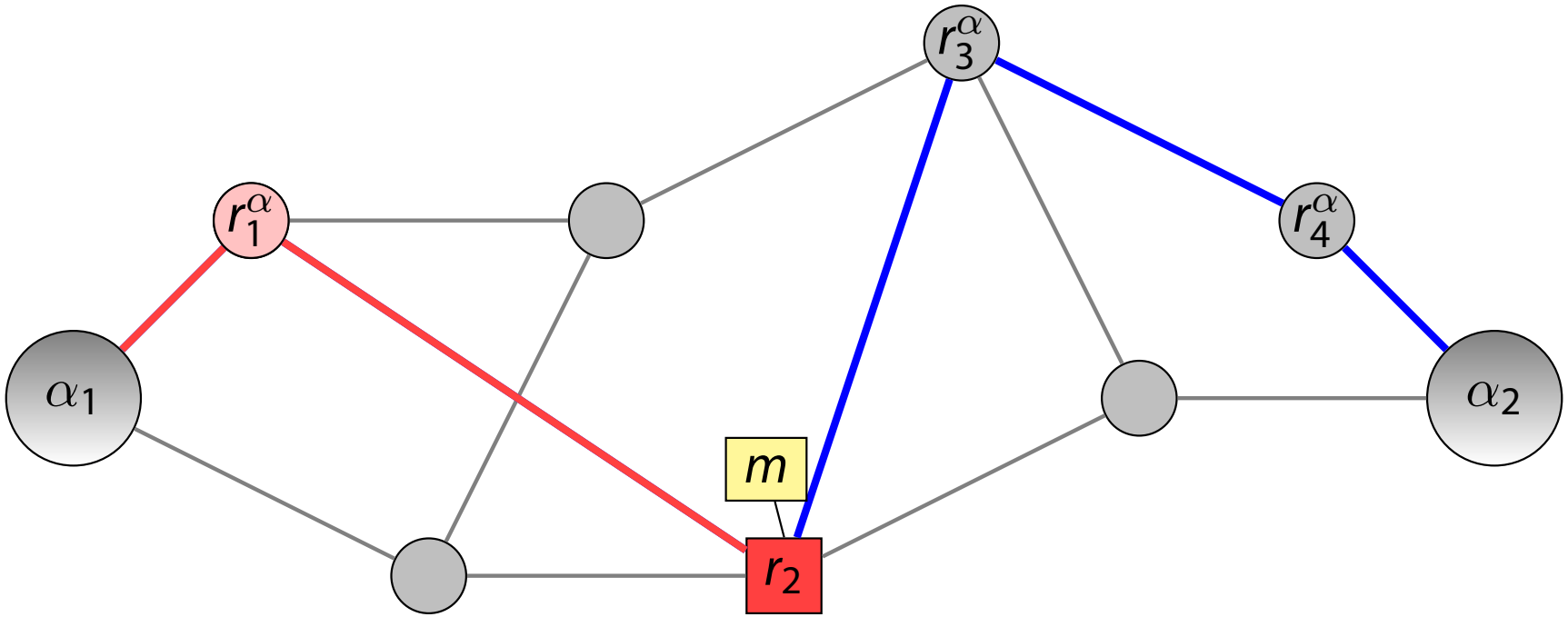
Was tut Alpha?



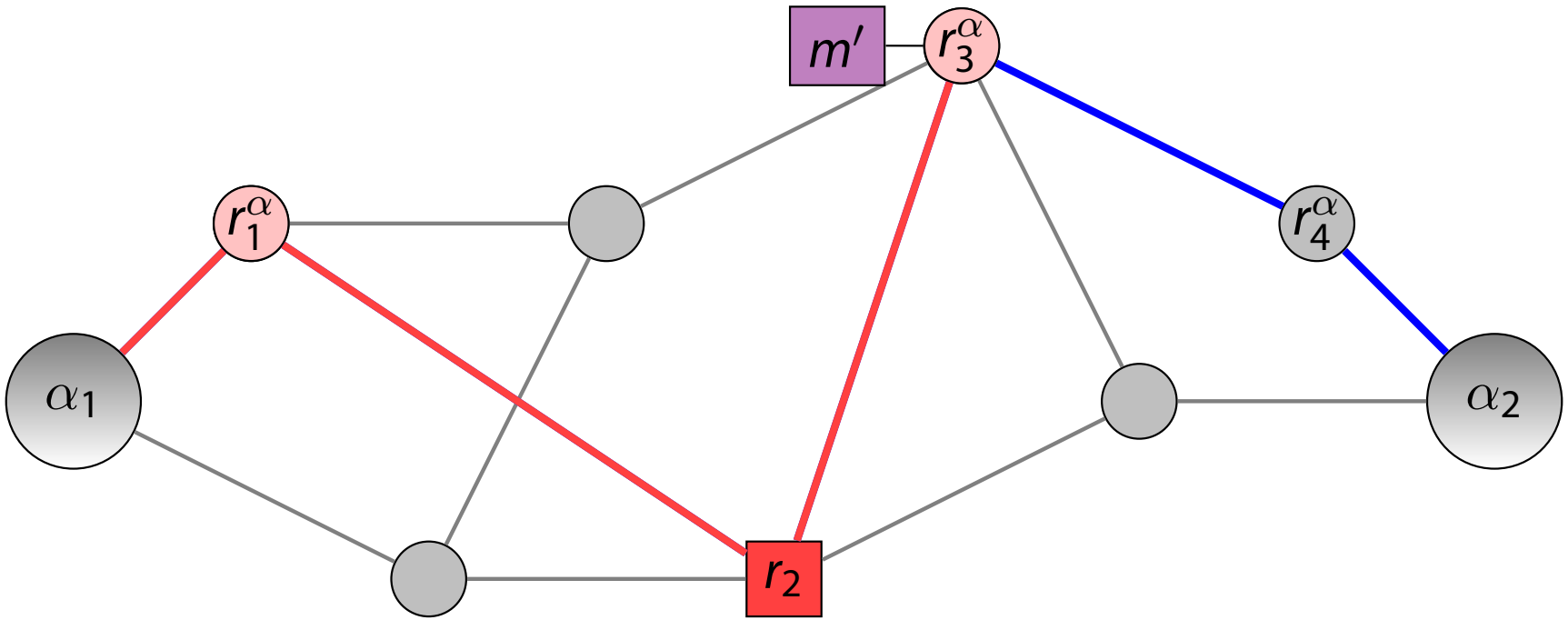
Was tut Alpha?



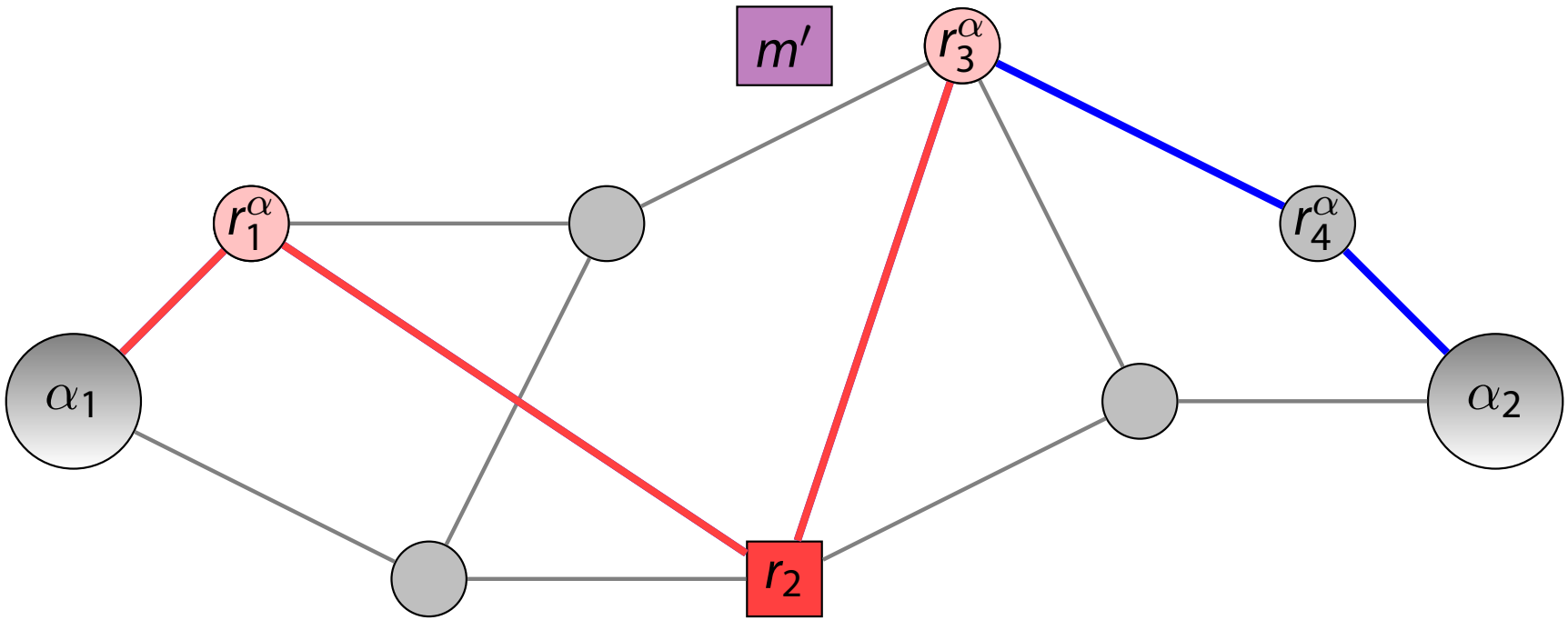
Was tut Alpha?



Was tut Alpha?



Was tut Alpha?



Was ist Alpha?

Grundlage

Heer, T., Götz, S., Morchon, O.G. und Wehrle, K.

***ALPHA**: An **A**daptive and **L**ightweight **P**rotocol for **H**op-by-Hop **A**uthentication*

Proceedings of the 2008 ACM CoNEXT Conference, 2008.

Was ist Alpha?

Grundlage

Heer, T., Götz, S., Morchon, O.G. und Wehrle, K.

***ALPHA**: An **A**daptive and **L**ightweight **P**rotocol for **H**op-by-Hop **A**uthentication*

Proceedings of the 2008 ACM CoNEXT Conference, 2008.

Bis zu diesem Zeitpunkt . . .

- Nur Theorie, keine Implementierung

Was ist Alpha?

Grundlage

Heer, T., Götz, S., Morchon, O.G. und Wehrle, K.

***ALPHA**: An **A**daptive and **L**ightweight **P**rotocol for **H**op-by-Hop **A**uthentication*

Proceedings of the 2008 ACM CoNEXT Conference, 2008.

Bis zu diesem Zeitpunkt . . .

- Nur Theorie, keine Implementierung

Was beinhaltet der Name?

- *Adaptive*: Flexibel bezogen auf verschiedene Anwendungsszenarien
- *Lightweight*: Algorithmen sind schnell genug für kleine Geräte
- *Hop-by-Hop*: Router können Echtheit jedes Pakets überprüfen

Was haben wir gemacht?

Unsere Aufgabe

- Das Alpha-Protokoll implementieren

Was haben wir gemacht?

Unsere Aufgabe

- Das Alpha-Protokoll implementieren

Genauer

- Alpha implementieren (Grundmodus)
- Alpha erweitern (weitere Modi)
- Plattformunabhängigkeit
- Alpha-Filter
- "Böser" Filter
- Dokumentation
- Testläufe

Funktionen

Kompatibilität

- Linux (End-Geräte und Router)
- Apple Mac OS X
- Nokia N800 Smartphones (Maemo Betriebssystem)
- Wahrscheinlich (fast) alle Unix BSD Systeme (nicht getestet)

Funktionen (2)

Betriebsmodi

- **N**: Grundmodus, geringe Verzögerung
- **C**: Kumulativer Modus, hohe Bandbreite
- **M**: Hohe Bandbreite, andere Speicheranforderungen als **C**

Funktionen (2)

Betriebsmodi

- **N**: Grundmodus, geringe Verzögerung
- **C**: Kumulativer Modus, hohe Bandbreite
- **M**: Hohe Bandbreite, andere Speicheranforderungen als **C**

Paketbearbeitung

- Unterschiedliche Kanäle (Assoziationen), mit eigenen Modi
- Scheduler (welches Paket geht zuerst raus?)
- Zeitüberschreitungen feststellen (wo gingen Pakete verloren?)

Probleme und Herausforderungen

Technisch

- Plattformunabhängigkeit
- Lückenhafte Dokumentation (Linux und Mac OS X Treiber)

Probleme und Herausforderungen

Technisch

- Plattformunabhängigkeit
- Lückenhafte Dokumentation (Linux und Mac OS X Treiber)

Organisatorisch

- Umfang des Quelltext wurde sehr groß (ca. 15.000 Zeilen)
- Konsistente und sinnvolle Dokumentation
- Testläufe mussten immer auf mind. 2 Computern gestartet werden
- Viel Funktionalität im Paper absichtlich nicht spezifiziert

Ausblick

Zukünftige Funktionen für Alpha

- Selbständiger und intelligenter Scheduler für Pakete
- Genauere Spezifikationen des Protokolls
- Alpha mit vielen Teilnehmern in der Praxis testen
- Alpha auf vielen anderen Gerätetypen laufen lassen

Ende

Vielen Dank für die Aufmerksamkeit!

Fragen?