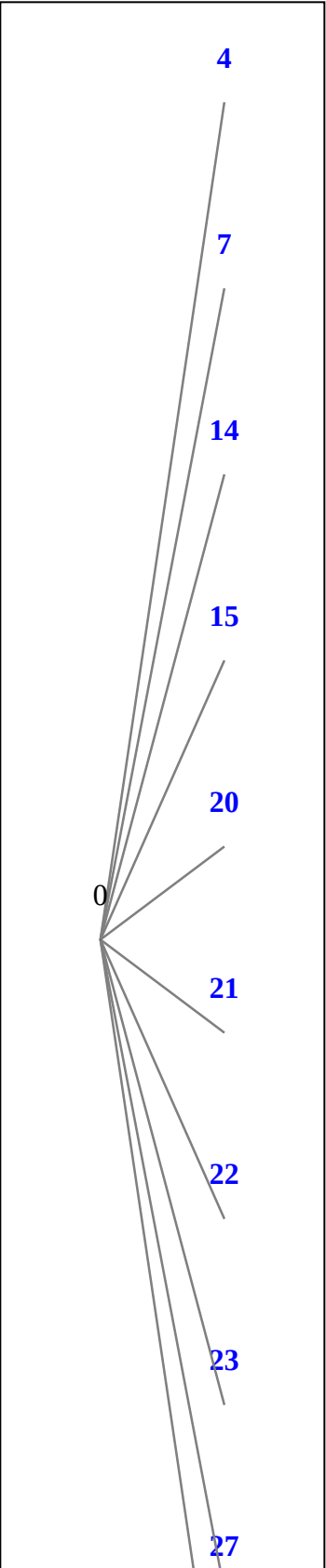
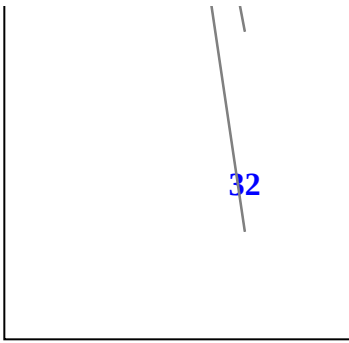


```
(comment "CPSA 3.6.6")  
(comment "Extracted shapes")  
(herald "Session Binding Protocol (SBP)")  
(comment "CPSA 3.6.6")  
(comment "All input read from sbp.lsp")
```

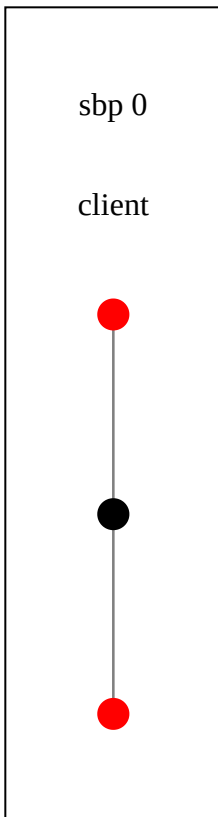
Tree 0.





```
(defprotocol sbp basic
  (defrole client
    (vars (answer2 cookie tlskey data) (proxy name))
    (trace (recv (enc cookie tlskey))
      (send (enc "request" cookie tlskey))
      (recv (enc "response2" answer2 cookie (privk proxy))))))
  (defrole proxy
    (vars (answer2 cookie tlskey data) (proxy name))
    (trace (send (enc cookie tlskey))
      (recv (enc "request" cookie tlskey))
      (send (enc "response2" answer2 cookie (privk proxy))))))
  (defrole server
    (vars (request2 answer answer2 cookie data))
    (trace (init (cat answer cookie))
      (tran (cat request2 cookie) answer2))))
```

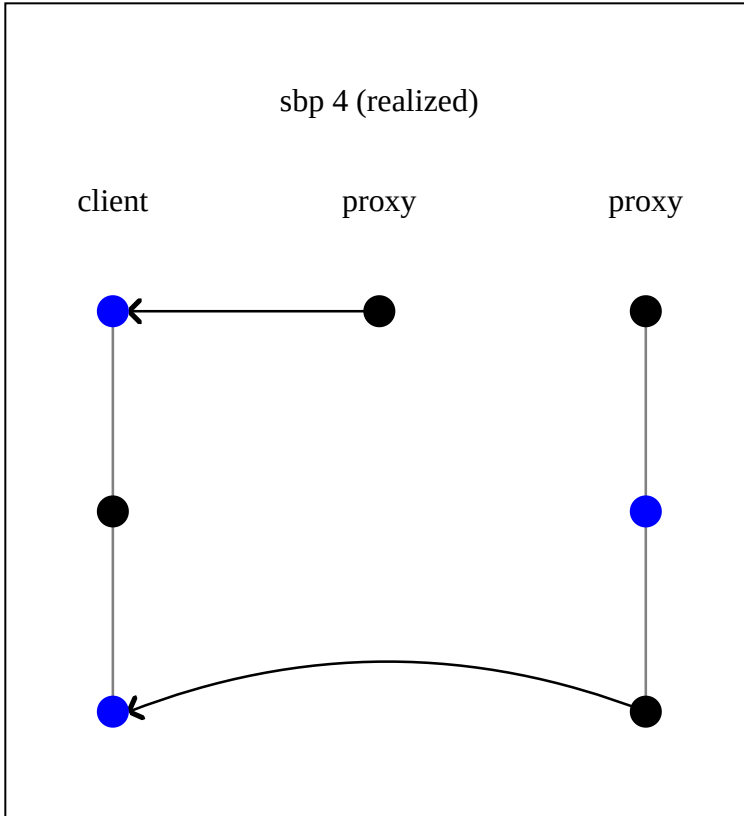
Item 0, Children: [4](#) [7](#) [14](#) [15](#) [20](#) [21](#) [22](#) [23](#) [27](#) [32](#).



```
(defskelton sbp
  (vars (tlskey answer2 cookie data) (proxy name))
  (defstrand client 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (non-orig (privk proxy))
  (pen-non-orig tlskey))
```

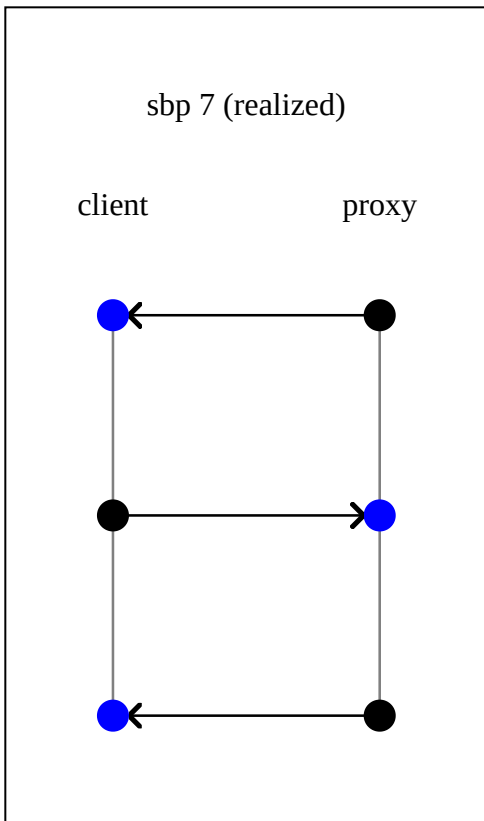
```
(label 0)
(unrealized (0 0) (0 2))
(origs)
(comment "2 in cohort - 2 not yet seen"))
```

Item [4](#), Parent: [0](#).



```
(defskeleton sbp
  (vars (tlskey answer2 cookie tlskey-0 data) (proxy name))
  (defstrand client 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 1 (cookie cookie) (tlskey tlskey))
  (defstrand proxy 3 (answer2 answer2) (cookie cookie) (tlskey tlskey-0)
    (proxy proxy))
  (precedes ((1 0) (0 0)) ((2 2) (0 2)))
  (non-orig (privk proxy))
  (pen-non-orig tlskey)
  (operation encryption-test (added-strand proxy 3)
    (enc "response2" answer2 cookie (privk proxy)) (0 2))
  (label 4)
  (parent 0)
  (unrealized)
  (shape)
  (maps
    ((0)
      ((proxy proxy) (tlskey tlskey) (answer2 answer2)
        (cookie cookie))))
  (origs))
```

Item [7](#), Parent: [0](#).

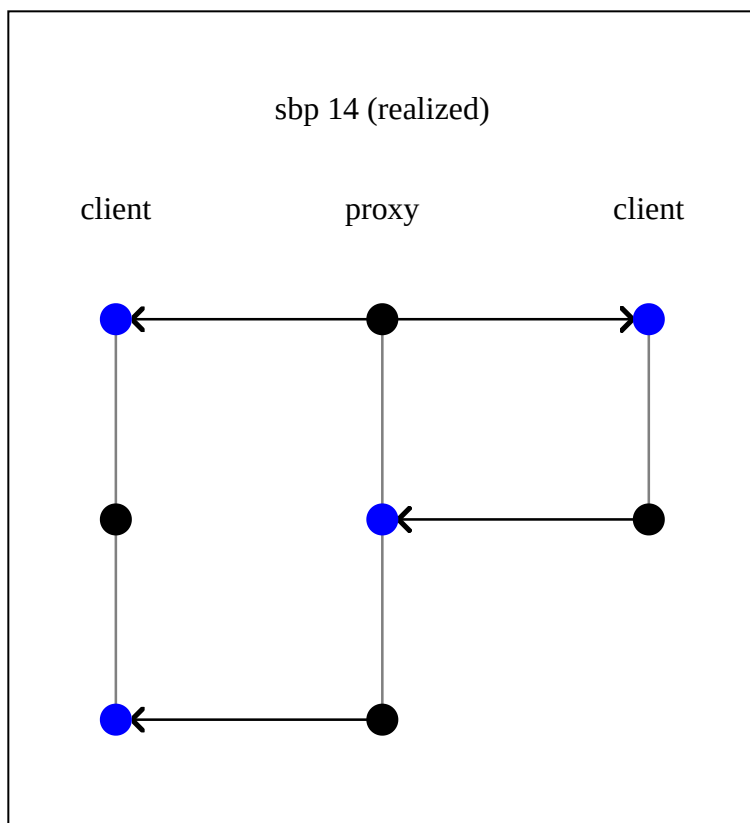


```

(defskeleton sbp
  (vars (answer2 cookie tlskey data) (proxy name))
  (defstrand client 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (precedes ((0 1) (1 1)) ((1 0) (0 0)) ((1 2) (0 2)))
  (non-orig (privk proxy))
  (pen-non-orig tlskey)
  (operation encryption-test (displaced 2 0 client 2)
    (enc "request" cookie tlskey) (1 1))
  (label 7)
  (parent 0)
  (unrealized)
  (shape)
  (maps
    ((0)
      ((proxy proxy) (tlskey tlskey) (answer2 answer2)
        (cookie cookie))))
  (origs))

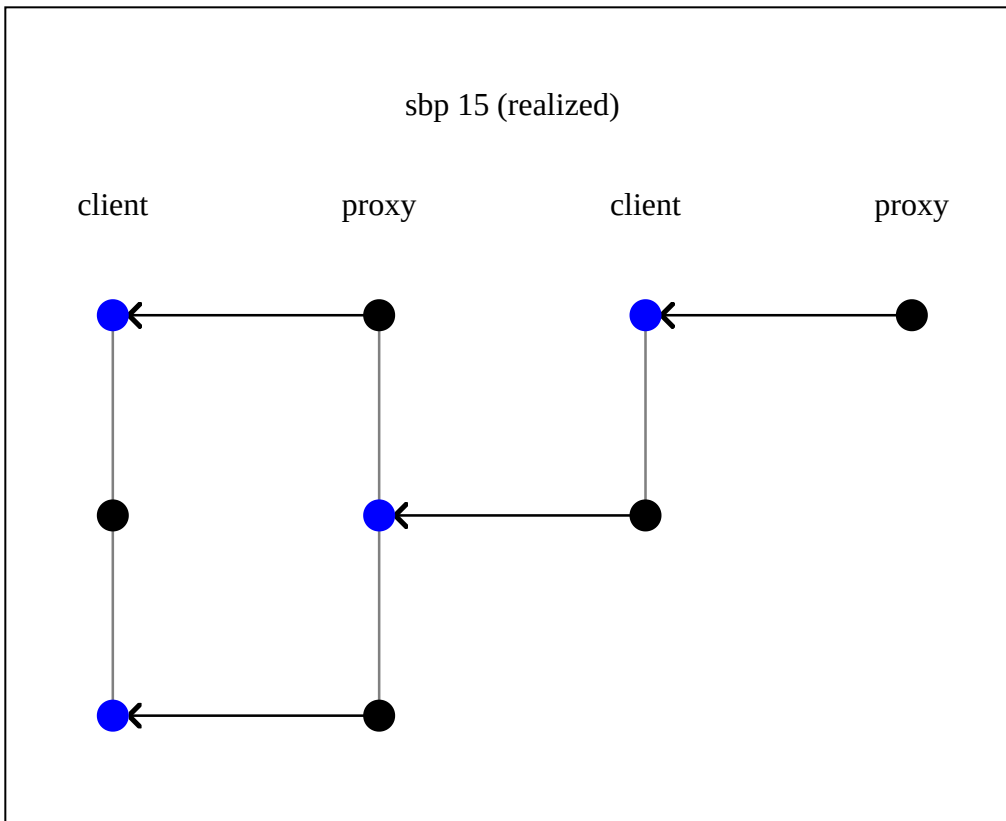
```

Item [14](#), Parent: [0](#).



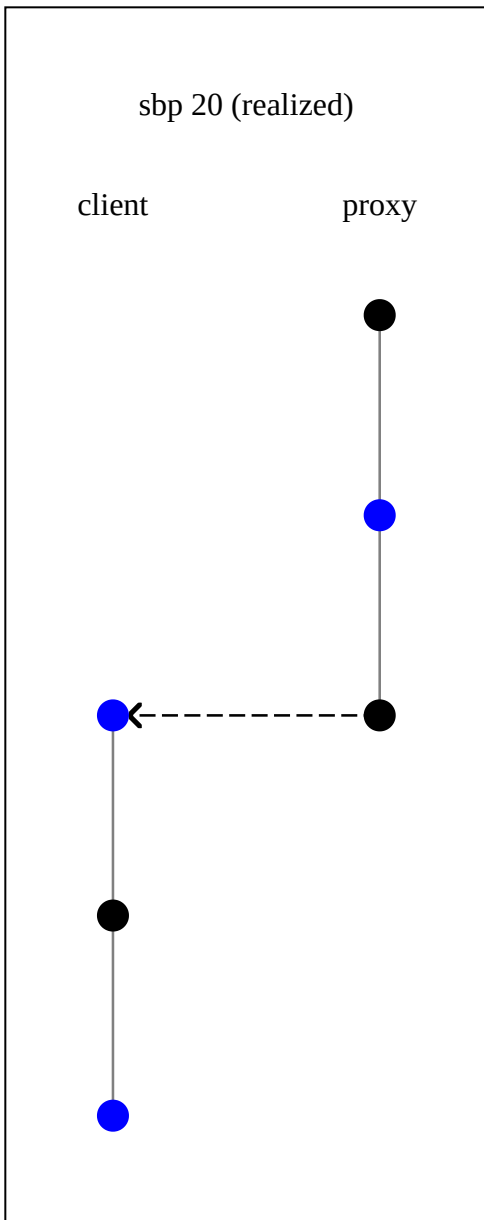
```
(defskelton sbp
  (vars (answer2 cookie tlskey data) (proxy name))
  (defstrand client 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand client 2 (cookie cookie) (tlskey tlskey))
  (precedes ((1 0) (0 0)) ((1 0) (2 0)) ((1 2) (0 2)) ((2 1) (1 1)))
  (non-orig (privk proxy))
  (pen-non-orig tlskey)
  (operation encryption-test (displaced 3 1 proxy 1) (enc cookie tlskey)
    (2 0))
  (label 14)
  (parent 0)
  (unrealized)
  (shape)
  (maps
    ((0)
      ((proxy proxy) (tlskey tlskey) (answer2 answer2)
        (cookie cookie))))
  (origs))
```

Item 15, Parent: 0.



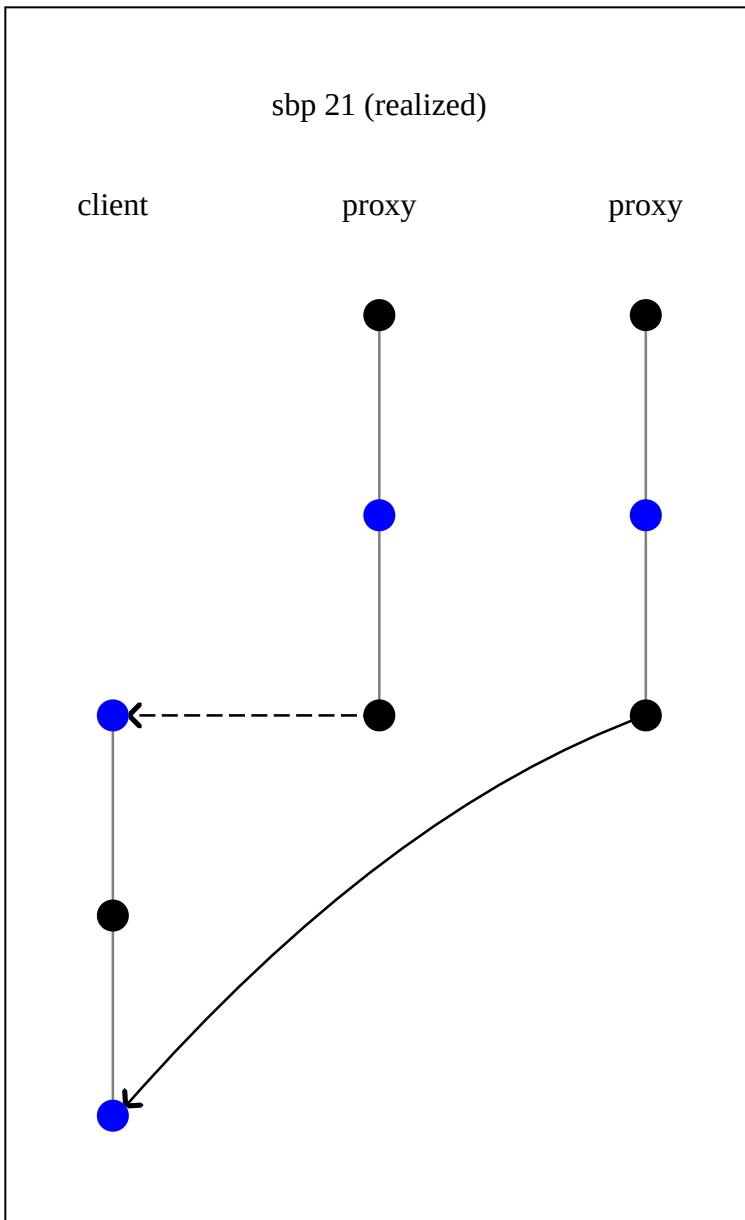
```
(defskeleton sbp
  (vars (answer2 cookie tlskey data) (proxy name))
  (defstrand client 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand client 2 (cookie cookie) (tlskey tlskey))
  (defstrand proxy 1 (cookie cookie) (tlskey tlskey))
  (precedes ((1 0) (0 0)) ((1 2) (0 2)) ((2 1) (1 1)) ((3 0) (2 0)))
  (non-orig (privk proxy))
  (pen-non-orig tlskey)
  (operation encryption-test (added-strand proxy 1) (enc cookie tlskey)
    (2 0))
  (label 15)
  (parent 0)
  (unrealized)
  (shape)
  (maps
    ((0)
      ((proxy proxy) (tlskey tlskey) (answer2 answer2)
        (cookie cookie))))
  (origs))
```

Item [20](#), Parent: [0](#).

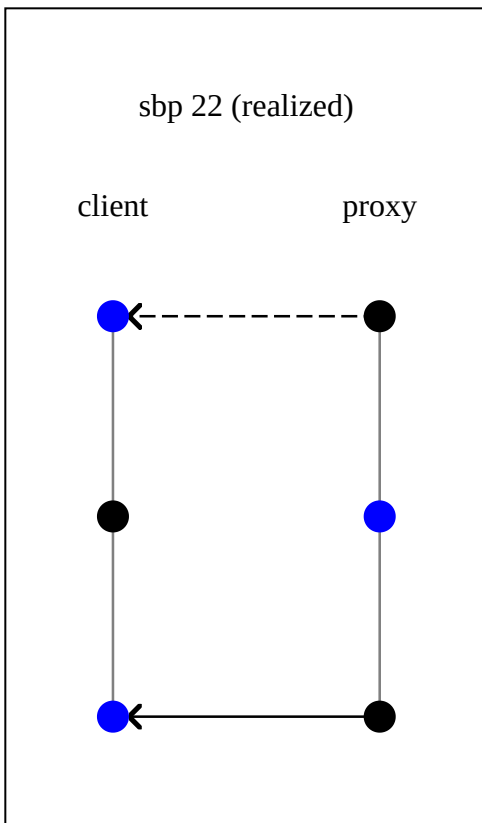


```
(defskeleton sbp
  (vars (tlskey cookie tlskey-0 data) (proxy name))
  (defstrand client 3 (answer2 tlskey) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 3 (answer2 tlskey) (cookie cookie) (tlskey tlskey-0)
    (proxy proxy))
  (precedes ((1 2) (0 0)))
  (non-orig (privk proxy))
  (pen-non-orig tlskey)
  (operation generalization deleted (1 0))
  (label 20)
  (parent 0)
  (unrealized)
  (shape)
  (maps
    ((0)
      ((proxy proxy) (tlskey tlskey) (answer2 tlskey) (cookie cookie))))
  (origs))
```

Item [21](#), Parent: [0](#).

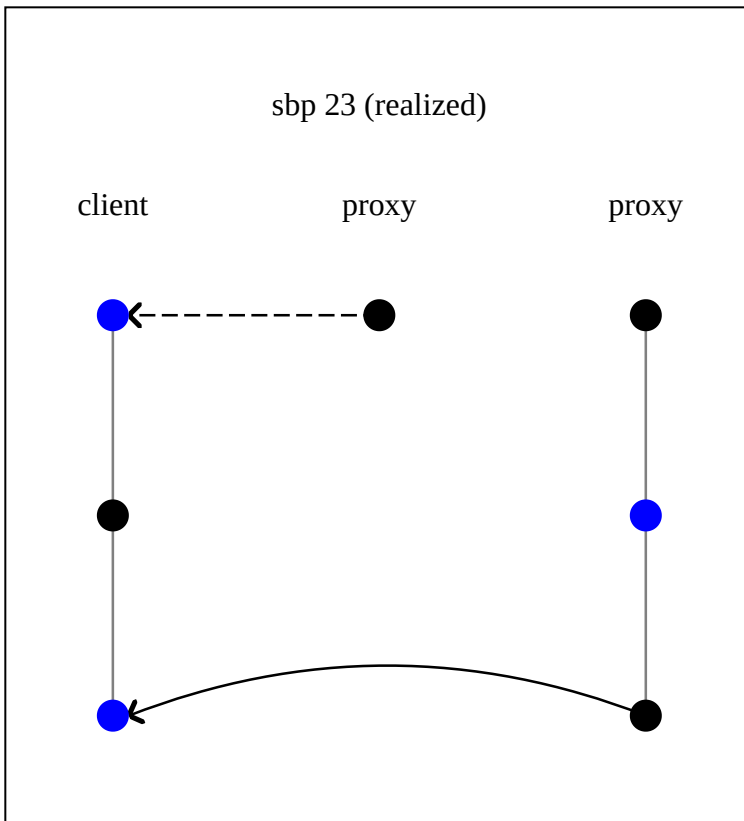


```
(defskeleton sbp
  (vars (tlskey answer2 cookie cookie-0 tlskey-0 tlskey-1 data)
    (proxy proxy-0 name))
  (defstrand client 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 3 (answer2 tlskey) (cookie cookie-0)
    (tlskey tlskey-0) (proxy proxy-0))
  (defstrand proxy 3 (answer2 answer2) (cookie cookie) (tlskey tlskey-1)
    (proxy proxy))
  (precedes ((1 2) (0 0)) ((2 2) (0 2)))
  (non-orig (privk proxy))
  (pen-non-orig tlskey)
  (operation generalization deleted (1 0))
  (label 21)
  (parent 0)
  (unrealized)
  (shape)
  (maps
    ((0)
      ((proxy proxy) (tlskey tlskey) (answer2 answer2)
        (cookie cookie))))
  (origs))
```


Item [22](#), Parent: [0](#).

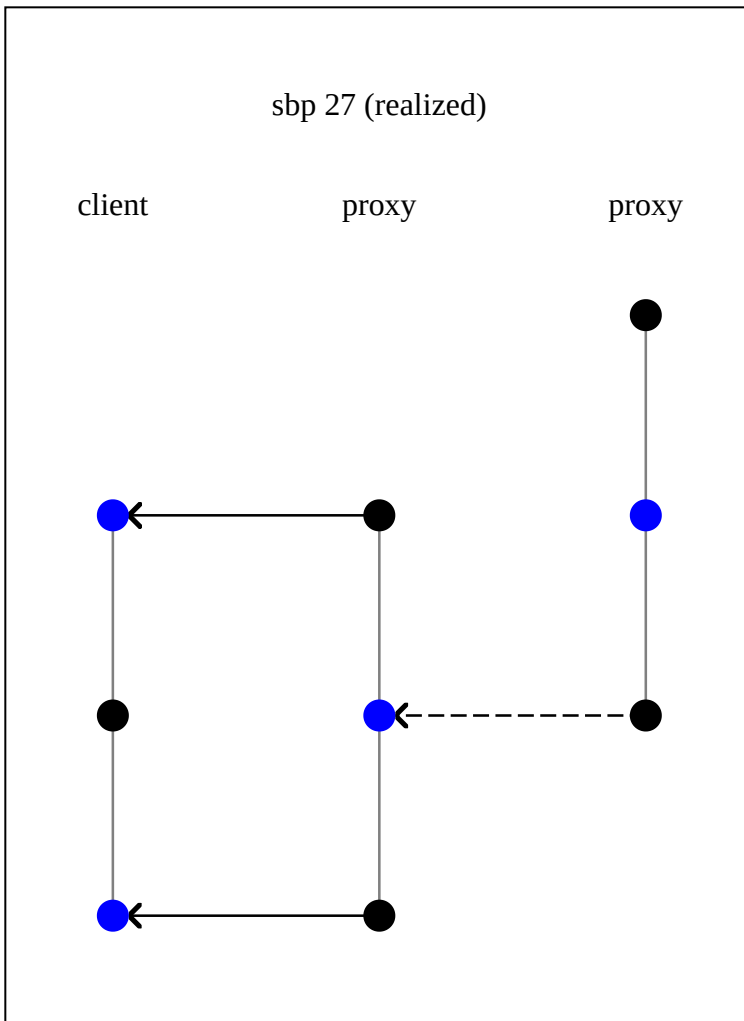
```
(defskeleton sbp
  (vars (answer2 cookie tlskey data) (proxy name))
  (defstrand client 3 (answer2 answer2) (cookie cookie) (tlskey cookie)
    (proxy proxy))
  (defstrand proxy 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (precedes ((1 0) (0 0)) ((1 2) (0 2)))
  (non-orig (privk proxy))
  (pen-non-orig cookie)
  (operation generalization deleted (1 0))
  (label 22)
  (parent 0)
  (unrealized)
  (shape)
  (maps
    ((0)
      ((proxy proxy) (tlskey cookie) (answer2 answer2)
        (cookie cookie))))
  (origs))
```

Item [23](#), Parent: [0](#).



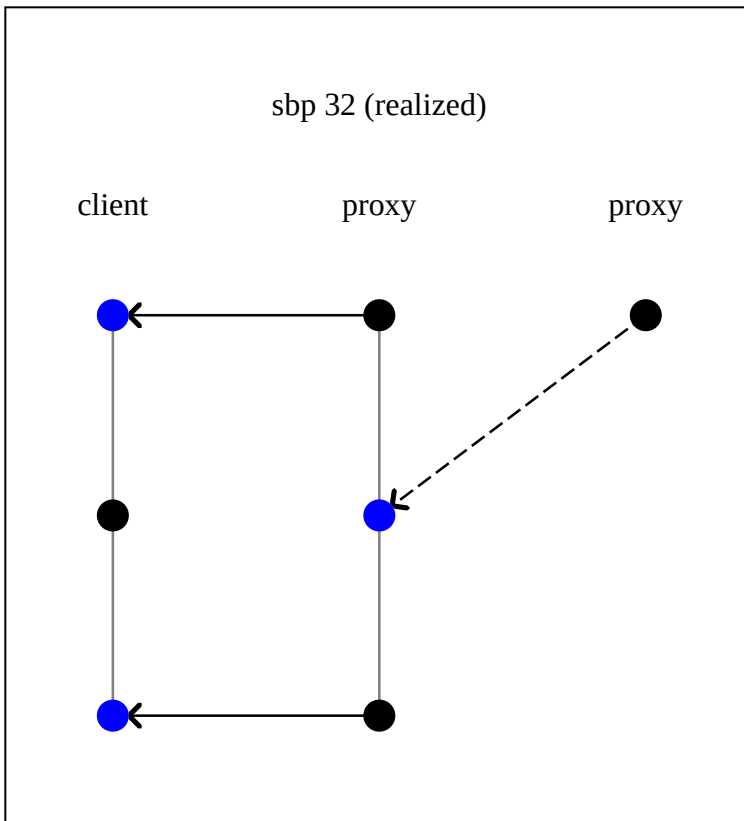
```
(defskeleton sbp
  (vars (tlskey answer2 cookie tlskey-0 tlskey-1 data) (proxy name))
  (defstrand client 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 1 (cookie tlskey) (tlskey tlskey-0))
  (defstrand proxy 3 (answer2 answer2) (cookie cookie) (tlskey tlskey-1)
    (proxy proxy))
  (precedes ((1 0) (0 0)) ((2 2) (0 2)))
  (non-orig (privk proxy))
  (pen-non-orig tlskey)
  (operation generalization deleted (1 0))
  (label 23)
  (parent 0)
  (unrealized)
  (shape)
  (maps
    ((0)
      ((proxy proxy) (tlskey tlskey) (answer2 answer2)
        (cookie cookie))))
  (origs))
```

Item [27](#), Parent: [0](#).



```
(defskeleton sbp
  (vars (answer2 cookie tlskey cookie-0 tlskey-0 data)
    (proxy proxy-0 name))
  (defstrand client 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 3 (answer2 tlskey) (cookie cookie-0)
    (tlskey tlskey-0) (proxy proxy-0))
  (precedes ((1 0) (0 0)) ((1 2) (0 2)) ((2 2) (1 1)))
  (non-orig (privk proxy))
  (pen-non-orig tlskey)
  (operation generalization deleted (2 0))
  (label 27)
  (parent 0)
  (unrealized)
  (shape)
  (maps
    ((0)
      ((proxy proxy) (tlskey tlskey) (answer2 answer2)
        (cookie cookie))))
  (origs))
```

Item [32](#), Parent: [0](#).



```
(defskeleton sbp
  (vars (answer2 cookie tlskey tlskey-0 data) (proxy name))
  (defstrand client 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 3 (answer2 answer2) (cookie cookie) (tlskey tlskey)
    (proxy proxy))
  (defstrand proxy 1 (cookie tlskey) (tlskey tlskey-0))
  (precedes ((1 0) (0 0)) ((1 2) (0 2)) ((2 0) (1 1)))
  (non-orig (privk proxy))
  (pen-non-orig tlskey)
  (operation generalization deleted (2 0))
  (label 32)
  (parent 0)
  (unrealized)
  (shape)
  (maps
    ((0)
      ((proxy proxy) (tlskey tlskey) (answer2 answer2)
        (cookie cookie))))
  (origs))
```