

## 1 A COUNTEREXAMPLE STATE IN THE NSPK PROTOCOL

The following is the counterexample state in the NSPK protocol found by Maude-NPA in Section 4 of the manuscript.

```
reduce in MAUDE-NPA : run(0, unbounded) .
result ShortIdSystem: < 1 . 5 . 2 . 7 . 2 . 4 . 2 . 1 > (
:: nil ::
[ nil |
  -(pk(i, n(b, #0:Fresh))),
  +(n(b, #0:Fresh)), nil] &
:: nil ::
[ nil |
  -(pk(i, a ; n(a, #1:Fresh))),
  +(a ; n(a, #1:Fresh)), nil] &
:: nil ::
[ nil |
  -(n(b, #0:Fresh)),
  +(pk(b, n(b, #0:Fresh))), nil] &
:: nil ::
[ nil |
  -(a ; n(a, #1:Fresh)),
  +(pk(b, a ; n(a, #1:Fresh))), nil] &
:: #1:Fresh ::
[ nil |
  +(pk(i, a ; n(a, #1:Fresh))),
  -(pk(a, n(a, #1:Fresh) ; n(b, #0:Fresh))),
  +(pk(i, n(b, #0:Fresh))), nil] &
:: #0:Fresh ::
[ nil |
  -(pk(b, a ; n(a, #1:Fresh))),
  +(pk(a, n(a, #1:Fresh) ; n(b, #0:Fresh))),
  -(pk(b, n(b, #0:Fresh))), nil] )
|
pk(a, n(a, #1:Fresh) ; n(b, #0:Fresh)) !inI,
pk(b, n(b, #0:Fresh)) !inI,
pk(b, a ; n(a, #1:Fresh)) !inI,
pk(i, n(b, #0:Fresh)) !inI,
pk(i, a ; n(a, #1:Fresh)) !inI,
n(b, #0:Fresh) !inI,
(a ; n(a, #1:Fresh)) !inI
|
+(pk(i, a ; n(a, #1:Fresh))),
-(pk(i, a ; n(a, #1:Fresh))),
+(a ; n(a, #1:Fresh)),
-(a ; n(a, #1:Fresh)),
+(pk(b, a ; n(a, #1:Fresh))),
```

```

-(pk(b, a ; n(a, #1:Fresh))),
+(pk(a, n(a, #1:Fresh) ; n(b, #0:Fresh))),
-(pk(a, n(a, #1:Fresh) ; n(b, #0:Fresh))),
+(pk(i, n(b, #0:Fresh))),
-(pk(i, n(b, #0:Fresh))),
+(n(b, #0:Fresh)),
-(n(b, #0:Fresh)),
+(pk(b, n(b, #0:Fresh))),
-(pk(b, n(b, #0:Fresh)))
|
nil

```

## 2 THE NUMBER OF STATES LOCATED AT EACH LAYER

The fourth column in Tables 1–2 shows the number of states located at each layer starting from depth zero up to the depth bound for each protocol, which is a list of natural numbers separated by commas. If the last value in the list is  $X$ , it means that there are  $X$  states located at the depth bound. Especially, if  $X$  is zero, it means that there is no state for the layer. If the last value in the list is of the form  $X + Y$ , it means that there are  $X + Y$  states located at the depth bound while  $Y$  is the number of initial states (counterexamples).

Table 1. The number of states located at each layer.

Protocol	Attack State	Depth	States located at layers (0, ..., i)
<b>1. Symmetric Key Protocols</b>			
Amended Needham Schroeder	0	7	1, 2, 4, 9, 26, 62, 152, 365 + 1
Carlsen Secret Key Initiator	0	5	1, 3, 8, 17, 40, 79 + 1
Denning Sacco	0	11	1, 1, 2, 3, 5, 7, 6, 5, 4, 3, 1, 0
Diffie Hellman	0	11	1, 4, 5, 9, 13, 18, 20, 22, 17, 12, 10, 5 + 1
	1	12	1, 6, 10, 11, 16, 20, 20, 21, 13, 9, 6, 3, 1 + 2
	2	13	1, 4, 6, 6, 7, 5, 3, 1, 0
ISO-5 Pass Authentication	0	5	1, 4, 4, 12, 23, 39 + 1
Kao-Chow RA	0	4	1, 3, 8, 17, 34 + 1
Kao-Chow RAHK	0	4	1, 1, 1, 2, 1, 0 + 1
Kao-Chow RAT	0	4	1, 2, 4, 14, 40 + 1
Otway-Rees	0	4	1, 2, 6, 15, 44 + 1
Secret 06	0	2	1, 2, 2 + 1
Secret 07	0	4	1, 4, 2, 1, 0 + 1
Wide Mouthed Frog	0	3	1, 5, 13, 26 + 1
Woo and Lam Authentication	0	4	1, 2, 2, 2, 0 + 2
Yahalom	0	4	1, 2, 8, 19, 30 + 1
<b>2. Homomorphism Protocols</b>			
Needham Schroeder Lowe ECB	0	7	1, 4, 9, 10, 5, 8, 14, 10 + 1
<b>3. Exclusive OR Protocols</b>			
Needham Schroeder Lowe XOR	0	8	1, 1, 2, 3, 3, 3, 2, 2, 2 + 1
SK3	0	3	1, 2, 1, 0
TMN Itv-F-tmn-asy	0	5	1, 4, 7, 8, 8, 6 + 1
WIRED Itv-C-wep-asy	0	5	1, 2, 1, 1, 1, 0
WIRED Itv-C-wep-variant	0	5	1, 2, 1, 1, 1, 0
<b>4. API Protocols</b>			
YubiKey	0	9	1, 1, 1, 2, 2, 1, 1, 1, 1, 0 + 1
	1	7	1, 4, 4, 9, 21, 88, 160, 0
	21	8	1, 4, 7, 16, 14, 2, 2, 5, 0
	3	7	1, 4, 4, 6, 18, 55, 80, 0
YubiHSM attack(d)	0	9	1, 1, 2, 3, 4, 7, 13, 24, 40, 75 + 1

Table 2. The number of states located at each layer.

Protocol	Attack State	Depth	States located at layers (0, ..., i)
<b>5. PKCS Protocols</b>			
PKCS11 a1-noComp	0	4	1, 3, 5, 7, 9 + 1
PKCS11 a2-noComp	0	6	1, 2, 2, 4, 11, 11, 4 + 1
PKCS11 a3-noComp	0	6	1, 3, 6, 13, 20, 21, 12 + 1
PKCS11 a4-noComp	0	7	1, 3, 7, 10, 10, 8, 6, 3 + 1
PKCS11 a5-noComp	0	9	1, 4, 11, 22, 31, 31, 15, 9, 5, 1 + 1
<b>6. Choice Protocols</b>			
encryption mode	0	4	1, 1, 1, 2, 3 + 1
	1	4	1, 2, 4, 8, 9 + 1
	2	10	1, 4, 9, 12, 15, 16, 13, 10, 6, 2, 0
	3	11	1, 4, 10, 18, 22, 24, 21, 18, 14, 8, 2, 0
rock paper scissors	0	9	1, 8, 16, 24, 27, 24, 18, 9, 3, 0
	1	1	1, 0
	2	2	1, 5, 0
TLS regular	0	3	1, 1, 1, 0 + 1
TLS attack	0	11	1, 4, 7, 10, 14, 18, 20, 24, 29, 35, 46, 69
<b>7. Distance-Bounding Protocols</b>			
brands chaum	1	4	1, 2, 3, 2, 0
	2	6	1, 3, 4, 3, 1, 1, 0 + 1
CRCS	1	9	1, 3, 8, 16, 26, 35, 28, 14, 4, 0
	2	8	1, 3, 3, 3, 6, 6, 3, 1, 0 + 1
H&K	1	5	1, 2, 4, 5, 2, 0
	2	2	1, 1, 0
MAD	1	9	1, 3, 7, 10, 10, 8, 5, 3, 1, 0
	2	6	1, 5, 10, 14, 18, 27, 40 + 1
Meadows v1-DH	1	4	1, 1, 1, 1, 0
	2	8	1, 2, 2, 3, 3, 3, 3, 1, 0
Meadows v2-DH	1	4	1, 1, 1, 1, 0
	2	3	1, 1, 1, 0 + 1
Munilla	1	7	1, 4, 7, 12, 22, 25, 10, 0
	2	4	1, 2, 2, 1, 0
Swiss Knife	1	4	1, 2, 3, 2, 0
	2	4	1, 4, 5, 2, 0
TREAD	1	4	1, 2, 3, 2, 0
	2	4	1, 3, 2, 1, 0 + 1