A trace has been found.

Abbreviations  $\sim M_2 2 = VERSION$   $\sim M_2 3 = CHALLENGE_AUTH$   $\sim M_2 4 = extLSB(hash(cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1))))$ 

~M\_25 = sign((hash(cert(IDPTx,spk(sskPTx),sign((IDPTx, spk(sskPTx)),sskCA\_1))),VERSION,CHALLENGE,nonce\_1, VERSION,CHALLENGE\_AUTH,extLSB(hash(cert(IDPTx, spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA\_1))))), sskPTx)

~X\_1 = (VERSION,CHALLENGE\_AUTH,~M\_24,~M\_25) = (VERSION, CHALLENGE\_AUTH,extLSB(hash(cert(IDPTx,spk(sskPTx), sign((IDPTx,spk(sskPTx)),sskCA\_1)))),sign((hash(cert(IDPTx,spk(sskPTx)),sign((IDPTx,spk(sskPTx)),sskCA\_1))),VERSION,CHALLENGE,nonce\_1,VERSION,CHALLENGE\_AUTH,extLSB(hash(cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA\_1)))),sskPTx))

		sskCA_1))),VERSION,CHALL extLSB(hash(cer	t(IDPTx,s Tx)),sskC
	Hones	st Process	Attac
	{1}nev	v sskCA_1	
		$\sim M = spk(sskCA_1)$	
		$\sim M_1 = spk(sskPTx)$	
	{7}new du	mmyIDPTx_1	
	{8}new dui	mmySskPTx_1	
		$\sim$ M_2 = spk(dummySskPTx_1)	<b>&gt;</b>
Beginning of proces	s PRx Beginning of process I	PTX	
		~M_3 = DigitalPing	-
		a	
		$\sim$ M_4 = SIG	-
	ID(~M_5,~M_6,~N	M_7,~M_8) = ID(MajorVer,MinorVer, MC,BDID)	-
		~M_9 = CFG	•
		a_1	
		$\sim$ M_10 = FOD	<b>→</b>
•		a_2	
		$\sim$ M_11 = SRQ	<b>▶</b>
		a_3	
		~M_12 = SRQen	•
		a_4	
		$\sim M 13 = CE$	
			<b>-</b>
		$\sim$ M_14 = RP	
{26} new nonce			
{26} new nonce			
{26} new nonce		$\sim$ M_14 = RP	
{26} new nonce		~M_14 = RP  7) = (VERSION,CHALLENGE,nonce_1)	
{26} new nonce		~M_14 = RP  7) = (VERSION,CHALLENGE,nonce_1)  a_5	
{26}new nonce		~M_14 = RP  7) = (VERSION,CHALLENGE,nonce_1)  a_5  a_6	
{26} new nonce		7) = (VERSION,CHALLENGE,nonce_1)  a_5  a_6  a_7	
{26} new nonce		~M_14 = RP  7) = (VERSION,CHALLENGE,nonce_1)  a_5  a_6  a_7  ~M_18 = ACK	
{26} new nonce		~M_14 = RP  7) = (VERSION,CHALLENGE,nonce_1)  a_5  a_6  a_7  ~M_18 = ACK  a_8	
{26} new nonce		~M_14 = RP  7) = (VERSION,CHALLENGE,nonce_1)  a_5  a_6  a_7  ~M_18 = ACK  a_8  ~M_19 = ACK	
{26} new nonce		~M_14 = RP  7) = (VERSION,CHALLENGE,nonce_1)  a_5  a_6  a_7  ~M_18 = ACK  a_8  ~M_19 = ACK  a_9	
{26} new nonce		~M_14 = RP  7) = (VERSION,CHALLENGE,nonce_1)  a_5  a_6  a_7  ~M_18 = ACK  a_8  ~M_19 = ACK  a_9  ~M_20 = ACK	
{26} new nonce		~M_14 = RP  7) = (VERSION,CHALLENGE,nonce_1)  a_5  a_6  a_7  ~M_18 = ACK  a_8  ~M_19 = ACK  a_9  ~M_20 = ACK  a_10	
{26} new nonce	(~M_15,~M_16,~M_1	~M_14 = RP  7) = (VERSION,CHALLENGE,nonce_1)  a_5  a_6  a_7  ~M_18 = ACK  a_8  ~M_19 = ACK  a_9  ~M_20 = ACK  a_10  ~M_21 = ACK	LENGE,
{26} new nonce	(~M_15,~M_16,~M_1	~M_14 = RP  7) = (VERSION, CHALLENGE, nonce_1)  a_5  a_6  a_7  ~M_18 = ACK  a_8  ~M_19 = ACK  a_9  ~M_20 = ACK  a_10  ~M_21 = ACK  a_11  a_12  DN, CHALLENGE, ~M_17) = (VERSION, CHALLENGE	LENGE,
{26}new nonce	(~M_15,~M_16,~M_1	~M_14 = RP  7) = (VERSION, CHALLENGE, nonce_1)  a_5  a_6  a_7  ~M_18 = ACK  a_8  ~M_19 = ACK  a_9  ~M_20 = ACK  a_10  ~M_21 = ACK  a_11  a_12  DN, CHALLENGE, ~M_17) = (VERSION, CHALLENGE	LENGE,