

Intro to Hash Signatures

Insecure OTS

h(Data)			
0	1	0	1
r0	r1	r2	r3
h(r0)	h(r1)	h(r2)	h(r3)
PK = h(h(R0) h(R1) h(R2) h(r3))			

Attack

H(Data)			
0	0	0	1
r0	r1	r2	r3
h(r0)	h(r1)	h(r2)	h(r3)
$PK = h(h(r0) h(r1) h(r2) h(r3))$			

Secure OTS

h(data)				number of 1's in hash	
0	1	0	1	1	0
r0	r1	r2	r3	c0	c1
h(r0)	h(r1)	h(r2)	h(r3)	h(c0)	h(c1)
PK = h(h(r0) h(r1) h(r2) h(r3) h(c0) h(c1))					

Blocked Attack

h(data)				number of 1's in hash	
0	0	0	1	0	1
r0	r1	r2	r3	c0	c1
h(r0)	h(r1)	h(r2)	h(r3)	h(c0)	h(c1)
$PK = h(h(r0) h(r1) h(r2) h(r3) h(c0) h(c1))$					

More Efficient OTS

h(data)				steps taken by signer	
“01”	“11”	“00”	“10”	“10”	“00”
r0	r1	r2	r3	c0	c1
$h^1(r0)$	$h^1(r1)$	$h^1(r2)$	$h^1(r3)$	$h^1(c0)$	$h^1(c1)$
$h^2(r0)$	$h^2(r1)$	$h^2(r2)$	$h^2(r3)$	$h^2(c0)$	$h^2(c1)$
$h^3(r0)$	$h^3(r1)$	$h^3(r2)$	$h^3(r3)$	$h^3(c0)$	$h^3(c1)$
PK = h(last row)					

Tree of “OTS”es

