H :
$\{0,1\}^* \rightarrow$
$\{0,1\}^n$
m
$H(m)$
$H(m)$
m
m'
$H(m) =$
$H(m')$
m,
m'
$H(m) =$
$H(m')$
m
$H(m)$
m
m
n
?
??
?
f
n
b
n
f
$\{0,1\}^n \times$
$\{0,1\}^{b-n} \rightarrow$
$\{0,1\}^n$
M
N
$b-$
n
f
H
f
IV
n
IV
$b-$
n
f
f
IV
f
?
2^{-38}
(M_0, M_0')
$(M_0) =(M_0')$
2^{39}
?
?
64
2012
?
$\emptyset$?
?
?
?
e
?
2015
3
?
?????
??????
2011
256
2012
4
224
256
?
3
384
512
2013
2
256
?
2016
2
3
224
256
384
512
4
?
2017
1
?
2019
3
224
$2^{39.39}$
4
224
256?
3
224
??
??
224/256/384/512 ?
224/256 2^{33} ?
224/256 ?