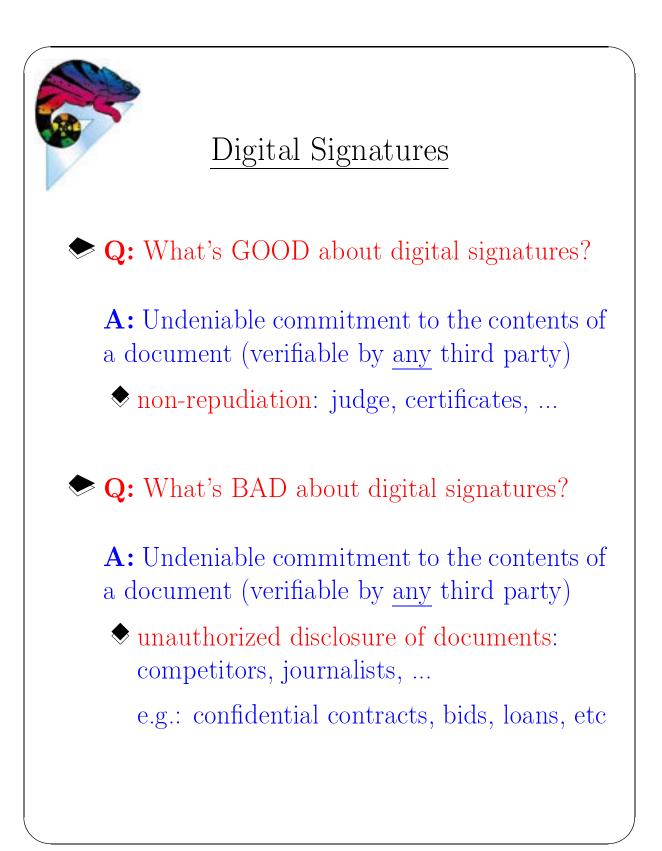


Hugo Krawczyk Tal Rabin

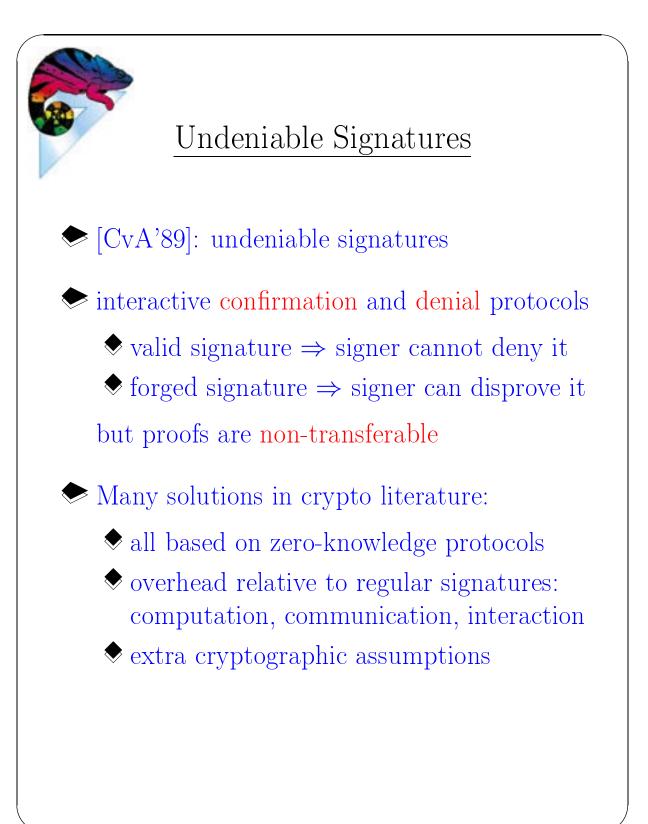
IBM T.J. Watson Research Center

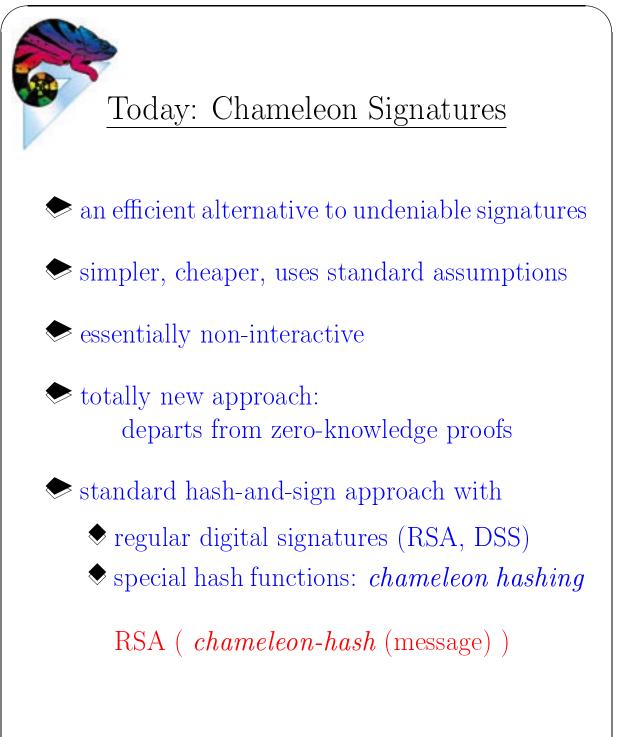


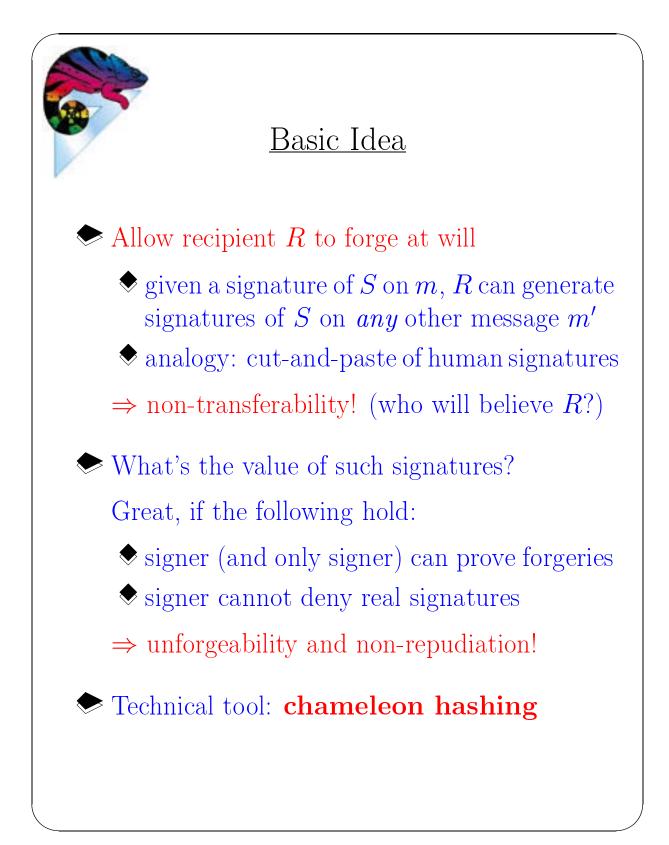
# Controlled Verification of Signatures

Conflicting requirements:

- $\blacklozenge$  Prevent disclosure to unauthorized parties
- $\clubsuit$  Be able to prove to a judge (to settle disputes)
- **Q:** Possible?
- A: Yes, if verification requires signer's action [CvA'89]







	<u>"Cut-and-Paste attack"</u>
Heptiu	Ltd. will supply 30 workstations m-NNY to Crooks Corp. between Jan- nd August 1999.
	John XYZ
	John XYZ
	Ltd. will invest 30 million dollars in 6 Corp. between January and June

## Reminder: collision-resistant hashing

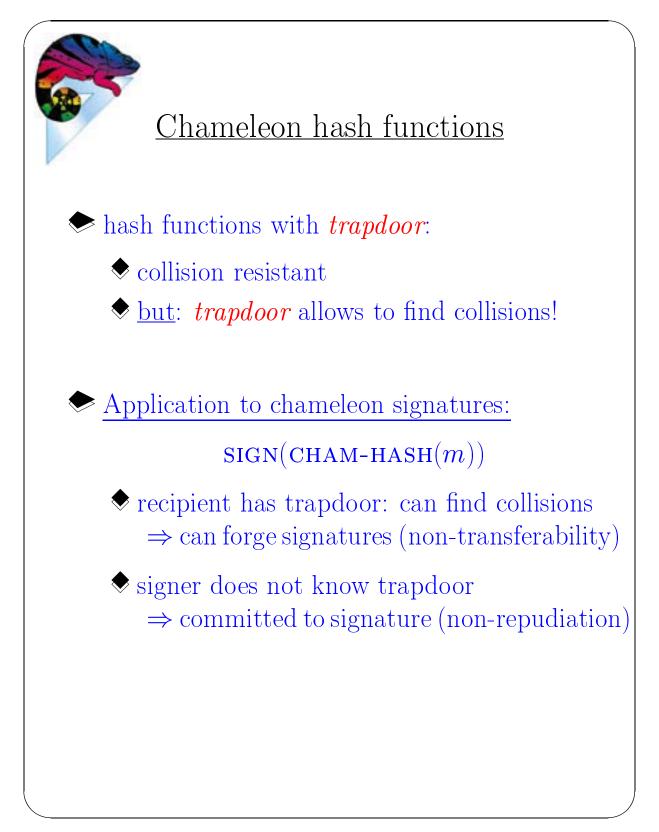
 $\blacklozenge$  no one can find two messages that are hashed to the same value

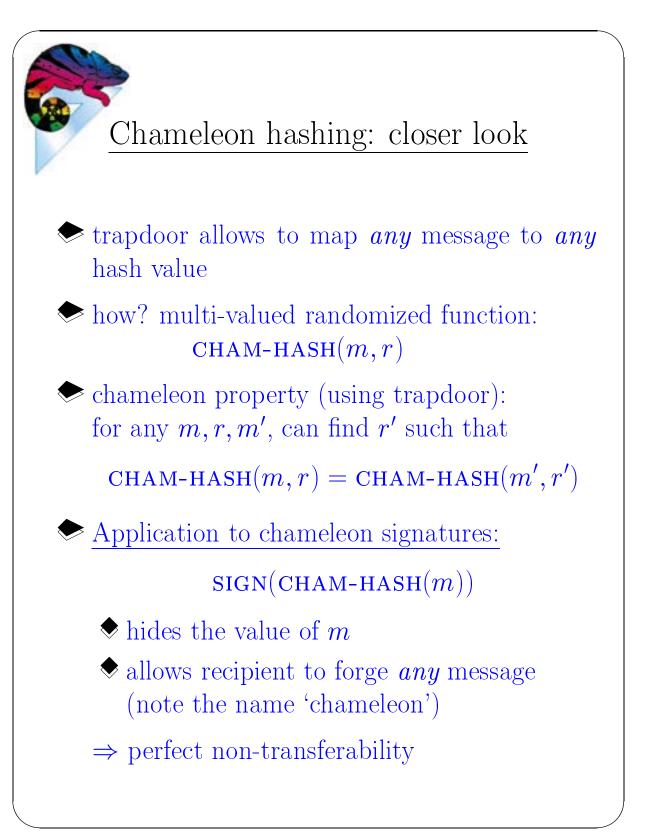
• instead of SIG(m) can do SIG(HASH(m))

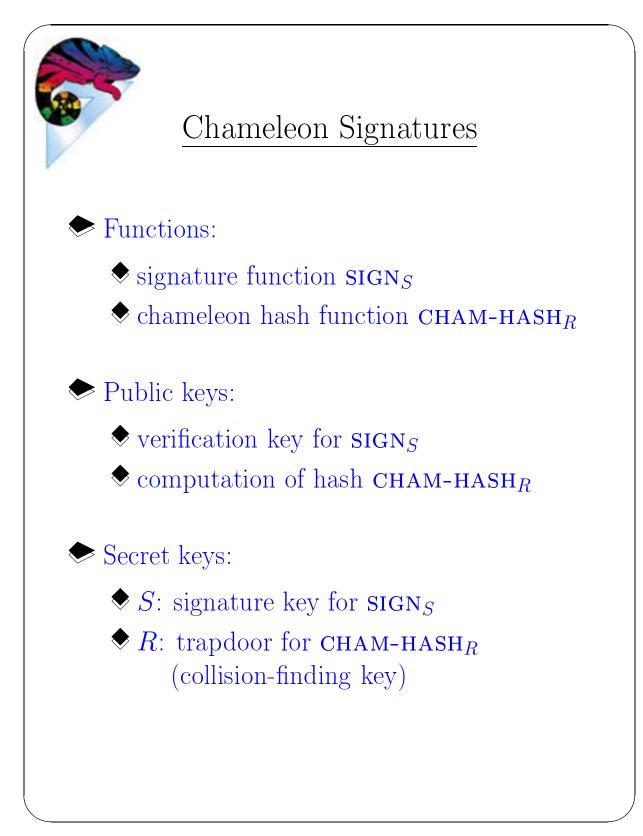
 $\blacklozenge$  resistance to collisions preserves unforgeability and non-repudiation

#### Note:

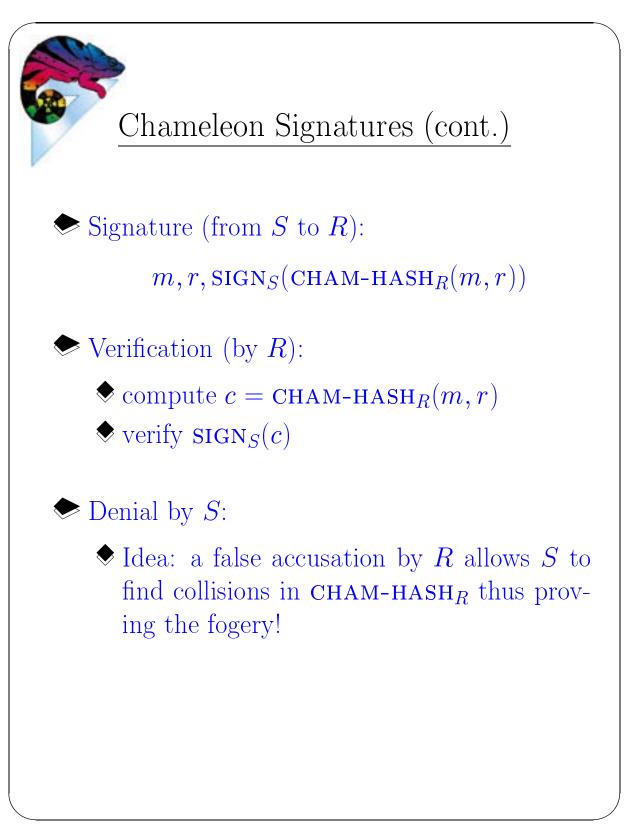
- if signer can find collisions then it can deny signatures
- if recipient can find collisions then it can forge signatures

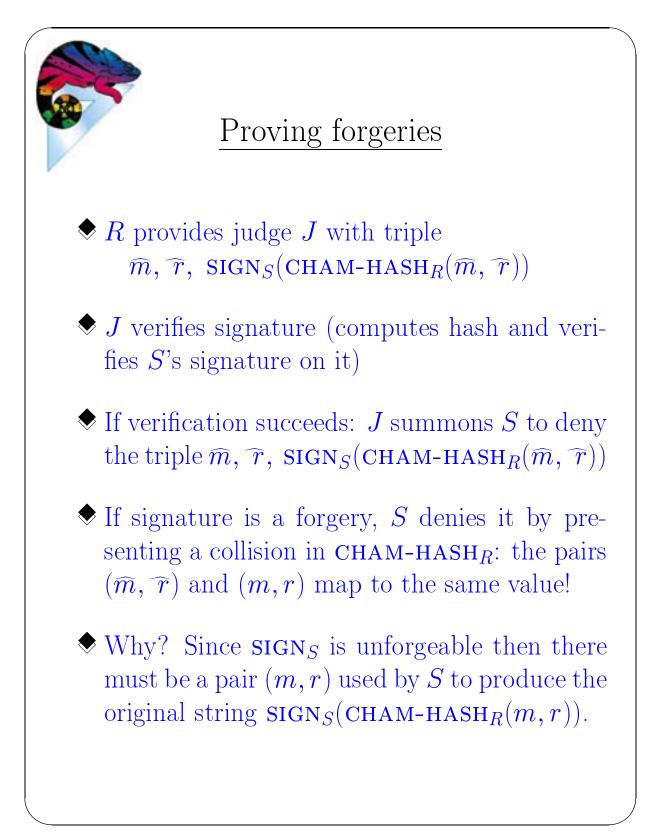


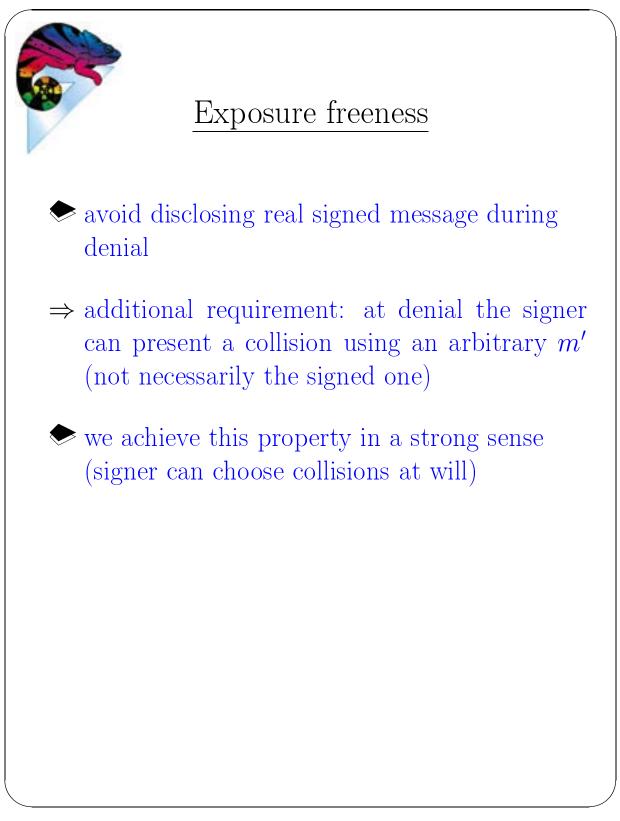




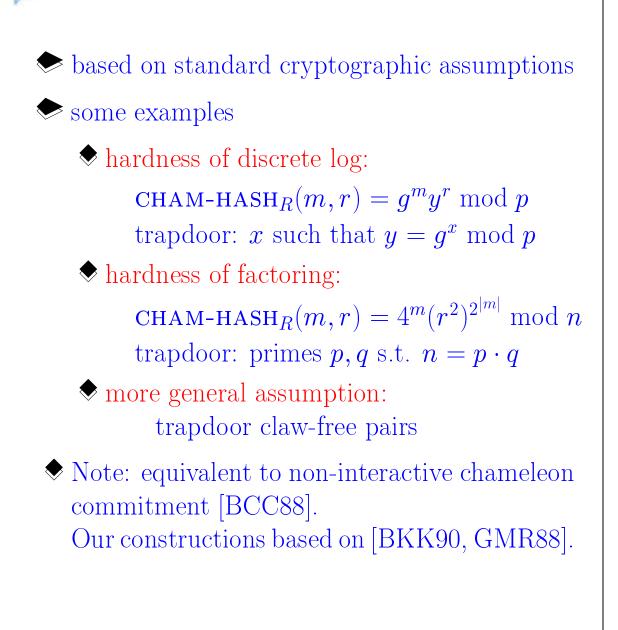
Page 10 of 17







## Implementation of Chameleon Hashing



## Discrete-log based Chameleon Hashing

### **Definition:**

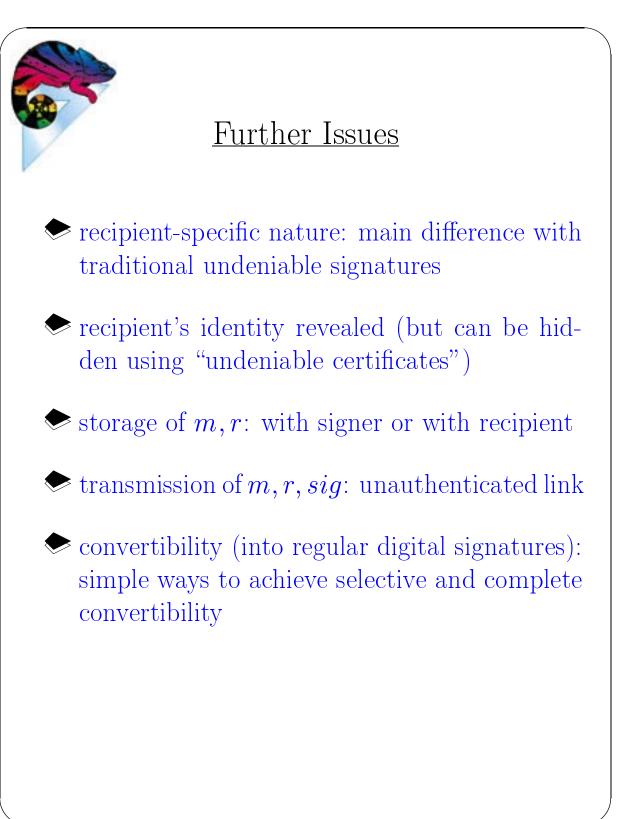
- $\blacklozenge$  primes p, q, p = kq + 1; g of order q in  $Z_p^*$
- $\blacklozenge$  trapdoor:  $x \in Z_q^*$ ; public key:  $y = g^x \mod p$
- ♦ hash: given m, choose random  $r \in Z_q^*$  and compute CHAM-HASH<sub>y</sub> $(m, r) = g^m y^r \mod p$
- $\diamond$  collision: m, r, m', r' with  $g^m y^r = g^{m'} y^{r'} \pmod{p}$

### **Properties:**

Collision resistance:  $finding collisions \Rightarrow computing disc-log (of y)
g^m y^r = g^{m'} y^{r'} \mod p \Rightarrow x = \frac{m - m'}{r' - r} \mod q.$ 

chameleon trapdoor: given m, r, m' can find  $r' \text{ as } r' = \frac{m + xr - m'}{x} \mod q$ 

denial: given collision (m, r) and  $(\widehat{m}, \widehat{r})$  can find  $x = \frac{m - \widehat{m}}{\widehat{r} - r} \mod q$  and with x can find collision with any other m' (exposure free).



## Summary and Conclusions

