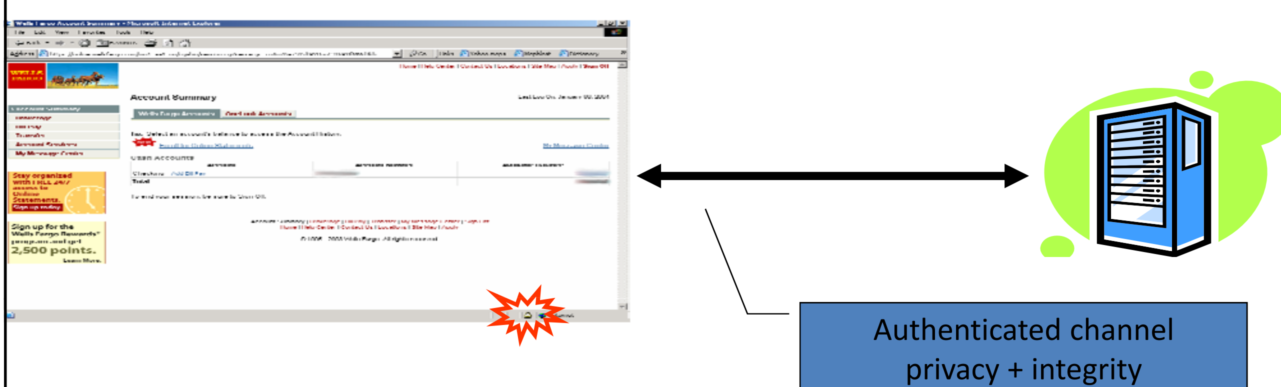
Software Security Foundations: *Crypto concepts II*

Dan Boneh, Stanford University

STANFORD UNIVERSITY
Stanford Center for Professional Development

Secure communication



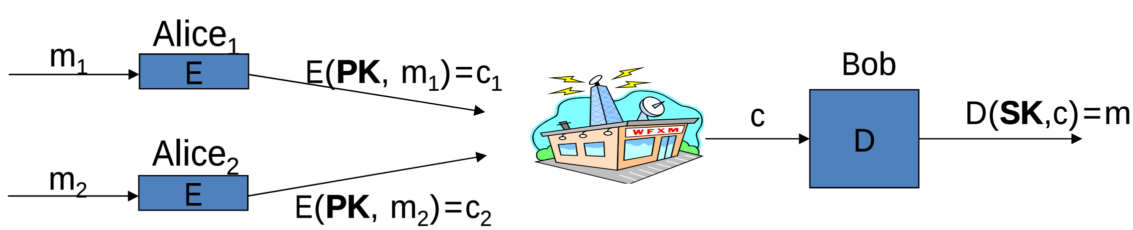
This segment: how do we generate session key?

Dan Boneh

Public key encryption

Public-key encryption

Tool for managing or generating symmetric keys



- E – Encryption alg. PK – Public encryption key
- D – Decryption alg. SK – Private decryption key

Algorithms E, D are publicly known.

Dan Boneh

Building block: trapdoor permutations

1. Algorithm KeyGen: outputs PK and SK

2. Algorithm $F(PK, \cdot)$: a one-way function
   - Computing $y = F(PK, x)$ is easy
   - One-way: given random y finding x is difficult

3. Algorithm $F^{-1}(SK, \cdot)$: Invert $F(PK, \cdot)$ using trapdoor SK

$$F^{-1}(SK, y) = x$$

Dan Boneh

Example: RSA

1. KeyGen: generate two equal length primes p, q

   set $N \leftarrow p \cdot q$ (3072 bits $\approx$ 925 digits)

   set $e \leftarrow 2^{16}+1 = 65537$; $d \leftarrow e^{-1} \pmod{\varphi(N)}$

   $PK = (N, e)$; $SK = (N, d)$

2. $RSA(PK, x)$: $x \rightarrow (x^e \bmod N)$

   Inverting this function is believed to be as hard as factoring N

3. $RSA^{-1}(SK, y)$: $y \rightarrow (y^d \bmod N)$

Dan Boneh

Public Key Encryption with a TDF

c_0	c_1

KeyGen: generate PK and SK

Encrypt(PK, M):
- choose random $x \in$ domain(F) and set $k \leftarrow H(x)$
- $c_0 \leftarrow F(PK, x)$, $c_1 \leftarrow E(k, M)$ (E: symmetric cipher)
- send $c = (c_0, c_1)$

Decrypt(SK, $c=(c_0,c_1)$): $x \leftarrow F^{-1}(SK, c_0)$, $k \leftarrow H(x)$, $M \leftarrow D(k, c_1)$

security analysis in crypto course

Dan Boneh

Digital Signatures

Digital signatures

Goal: bind document to author

- Problem: attacker can copy Alice's sig from one doc to another

Main idea: make signature depend on document

Example: signatures from trapdoor functions (e.g. RSA)

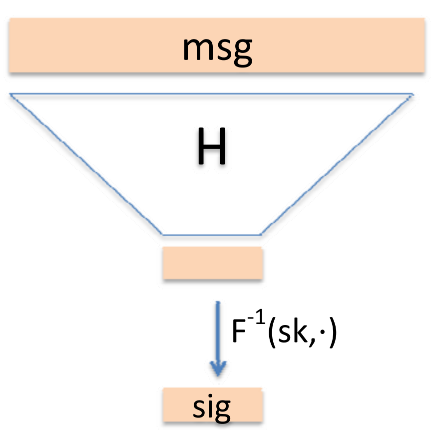
sign(SK, m) := F^{-1} (SK, H(m))

verify(PK, m, sig) := accept if F(PK, sig) = H(m)

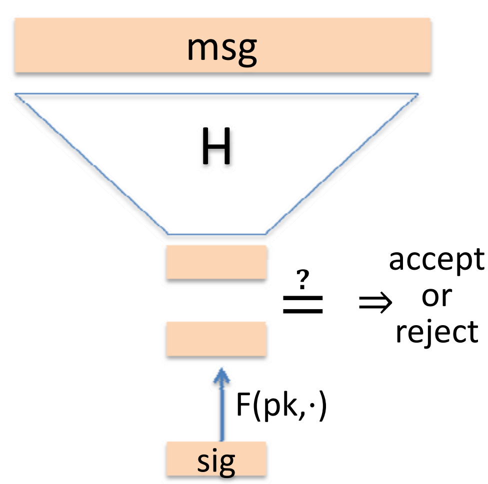
Dan Boneh

Digital Sigs. from Trapdoor Functions

sign(sk, msg):



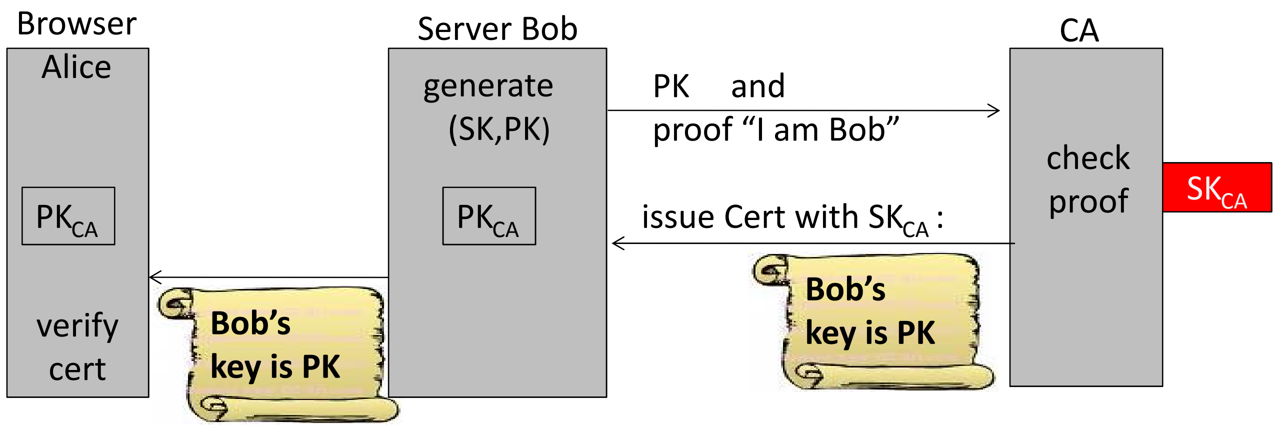
verify(pk, msg, sig):



Dan Boneh

Certificates: bind Bob's ID to his PK

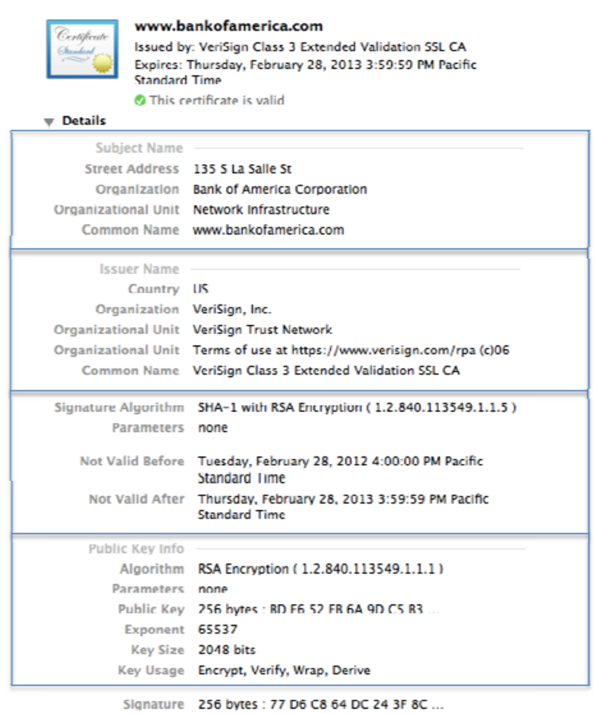
How does Alice (browser) obtain Bob's public key PK_{Bob} ?



Bob uses Cert for an extended period (e.g. one year)

Dan Boneh

Sample certificate:



www.bankofamerica.com
Issued by: VeriSign Class 3 Extended Validation SSL CA
Expires: Thursday, February 28, 2013 3:59:59 PM Pacific Standard Time
This certificate is valid

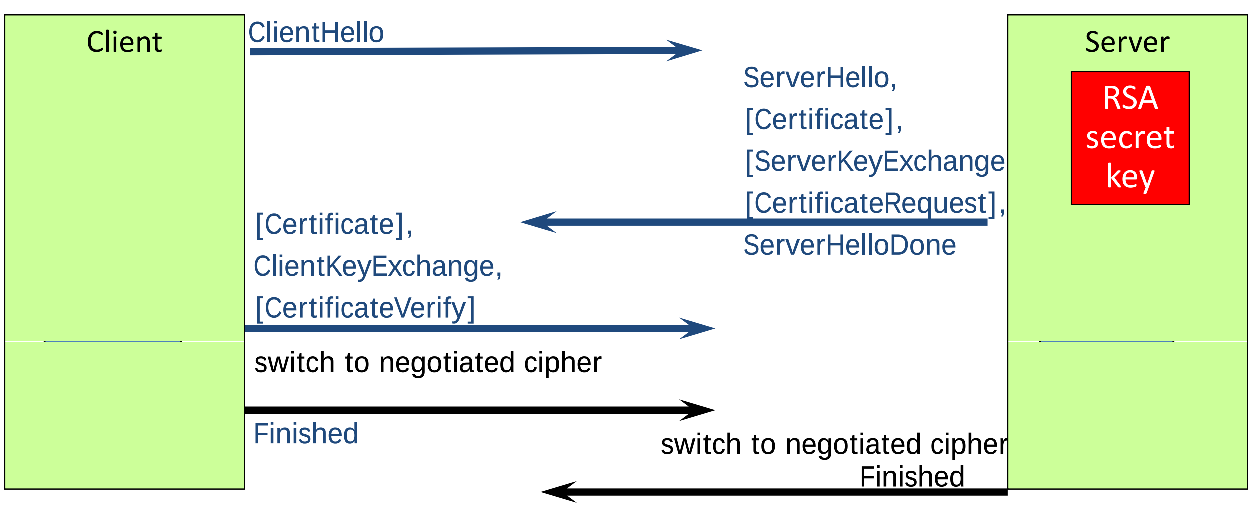
Details

Subject Name	
Street Address	135 S La Salle St
Organization	Bank of America Corporation
Organizational Unit	Network Infrastructure
Common Name	www.bankofamerica.com
Issuer Name	
Country	US
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)06
Common Name	VeriSign Class 3 Extended Validation SSL CA
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday, February 28, 2012 4:00:00 PM Pacific Standard Time
Not Valid After	Thursday, February 28, 2013 3:59:59 PM Pacific Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : BD F6 52 FB 6A 9D C5 B3 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	256 bytes : 77 D6 C8 64 DC 24 3F 8C ...

Dan Boneh

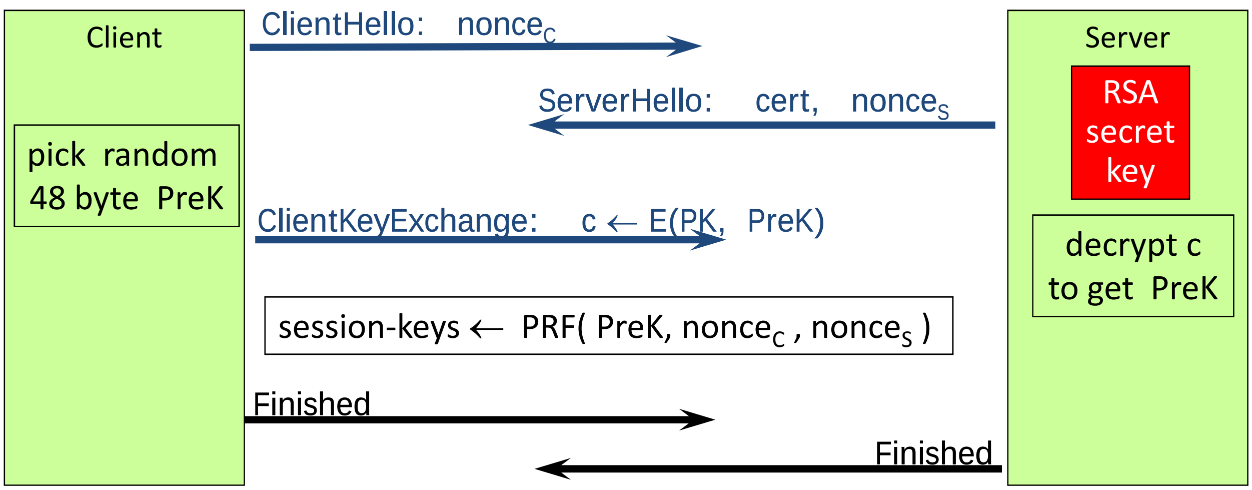
Schematic SSL session setup

Back to TLS session setup



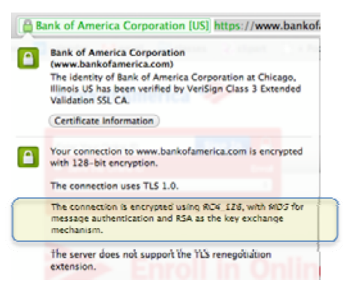
Dan Boneh

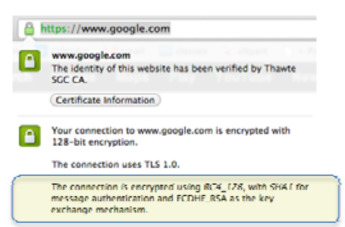
Abstract TLS (simplified)



Dan Boneh

Properties





Nonces: prevent replay of an old session

No forward secrecy:

– Compromise of server secret key exposes old sessions
– TLS has support for forward secrecy

One sided identification:

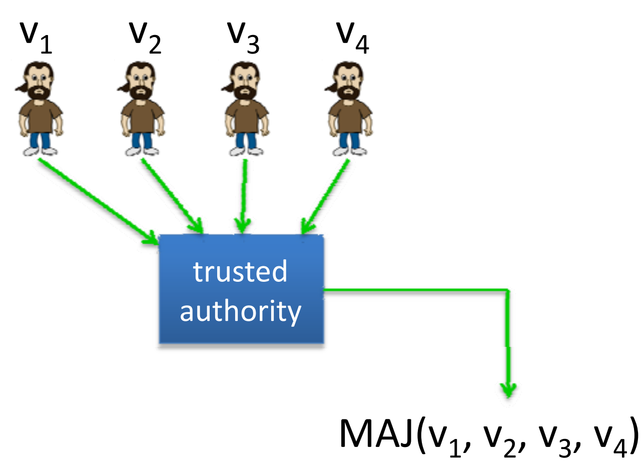
– Browser identifies server using server-cert
– TLS has support for mutual identification
  • Rarely used: requires a client PK/SK and client-cert

Dan Boneh

A Brief Overview of Modern Crypto Tools

Protocols

- Elections

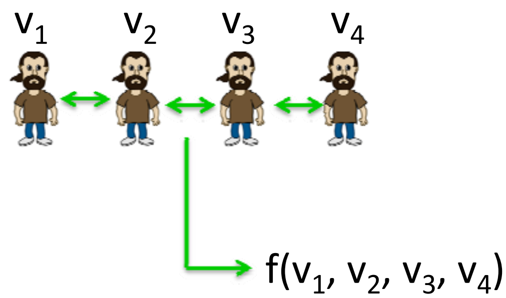


Can we do the same without a trusted party?

Dan Boneh

Protocols

- Elections
- Private auctions



Goal: compute $f(v_1, v_2, v_3, v_4)$

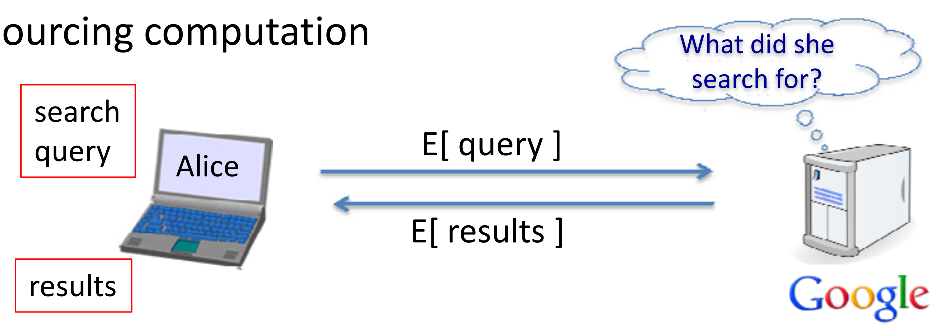
"Thm:" anything the can done with trusted auth. can also be done without

- Secure multi-party computation

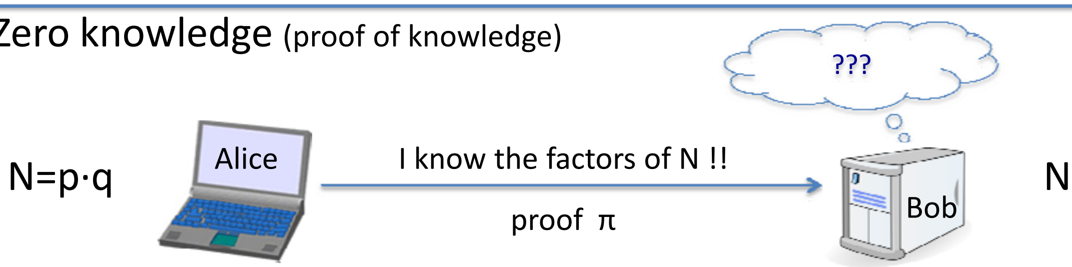
Dan Boneh

Magical applications

- Privately outsourcing computation

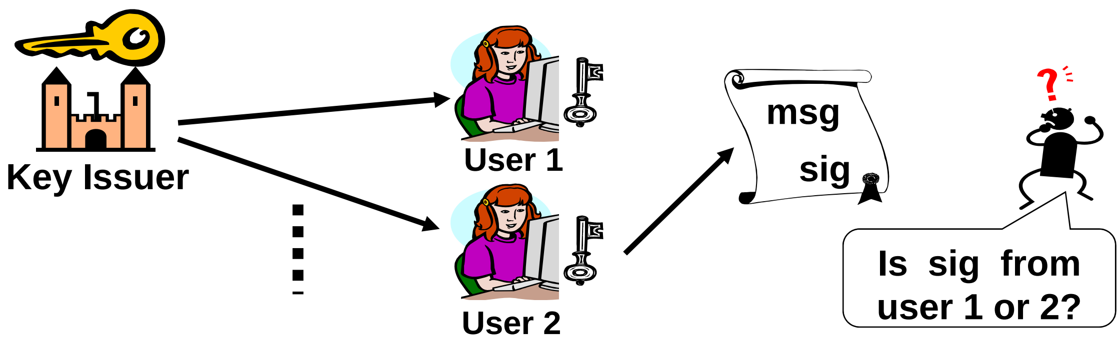


- Zero knowledge (proof of knowledge)



Dan Boneh

Privacy: Group Signatures



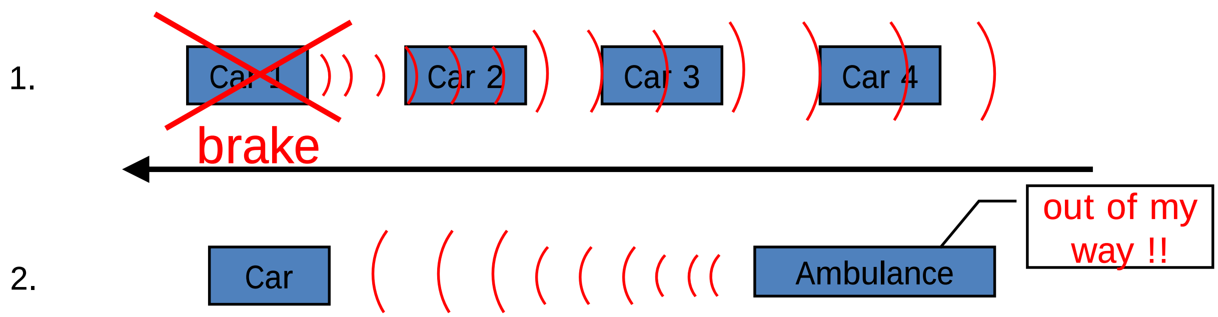
Simple solution: give all users same private key, but also need to:

– revoke signers when needed, and

– trace: trapdoor for undoing sig privacy.

Dan Boneh

Example: Vehicle Safety Comm. (VSC)



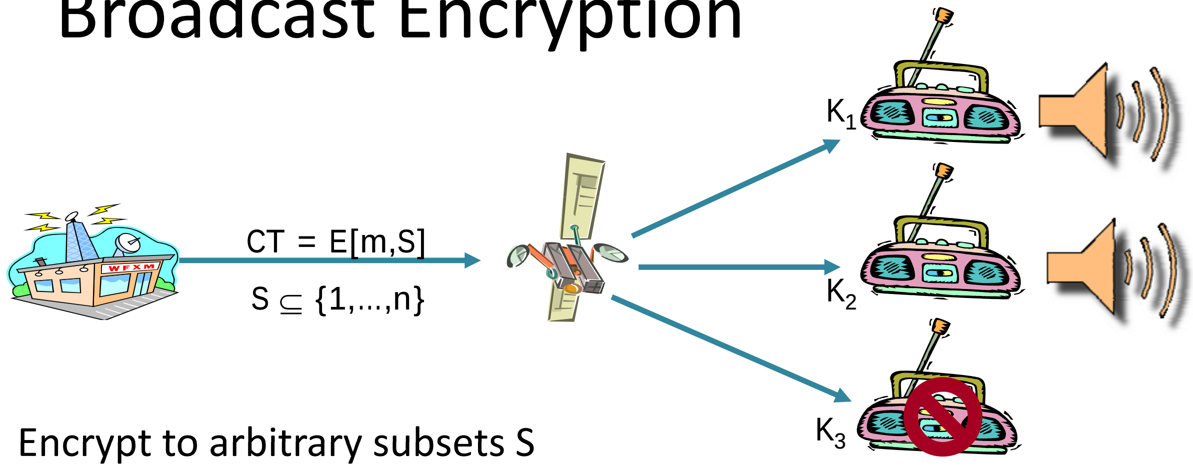
Require authenticated (signed) messages from cars.

– Prevent impersonation and DoS on traffic system.

Privacy problem: cars broadcasting signed (x,y, **V**).

Clean solution: group sigs. Group = set of all cars.

Broadcast Encryption



- Encrypt to arbitrary subsets S
- Short ciphertexts
- Collusion resistance: secure even if all users in S^c collude

Dan Boneh

Summary

RSA Trapdoor permutation:

- Enables public-key encryption and digital signatures
- Used in TLS session setup

Certificates:

- Bind public key to an identity
- Used in TLS to identify server (and possibly client)

Modern crypto: goes far beyond basic encryption and signatures

Dan Boneh