Bi-Deniable Encryption

Adam O'Neill Chris Peikert

Georgia Institute of Technology

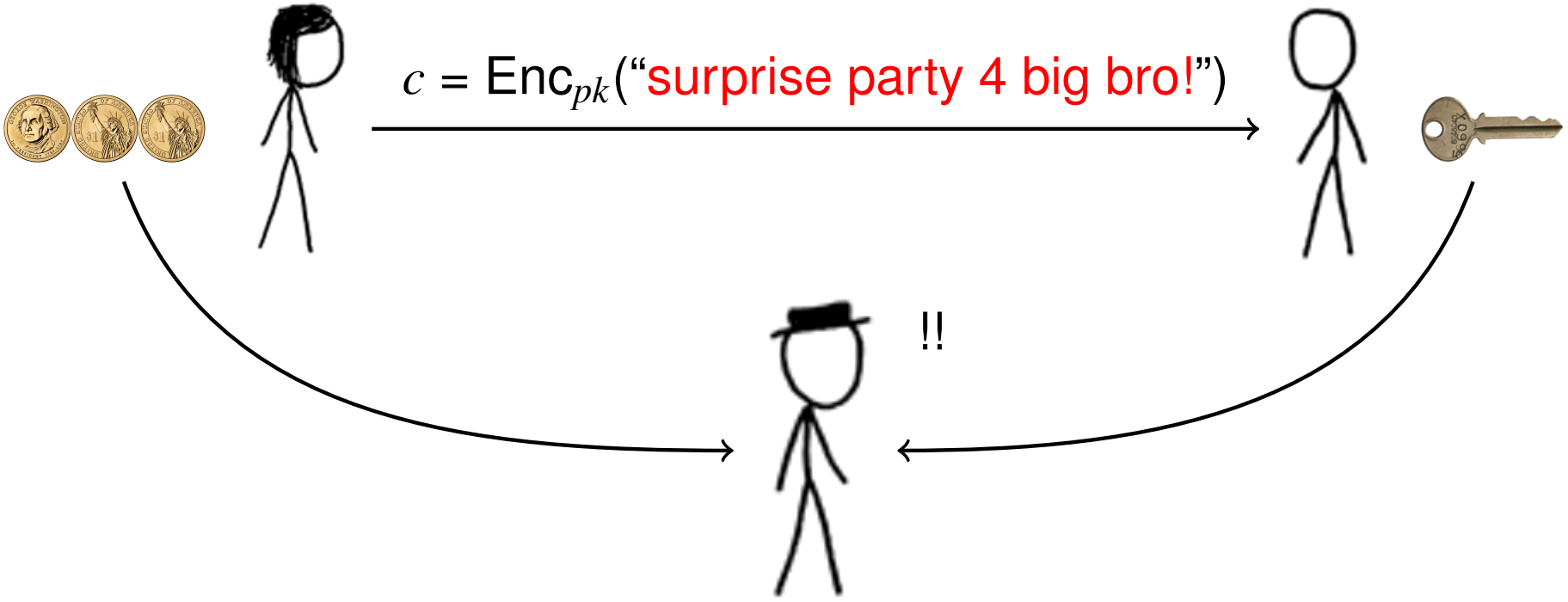
Eurocrypt 2010 Rump Session

Deniable Encryption

$c = \mathrm{Enc}_{pk}(\text{“surprise party 4 big bro!”})$

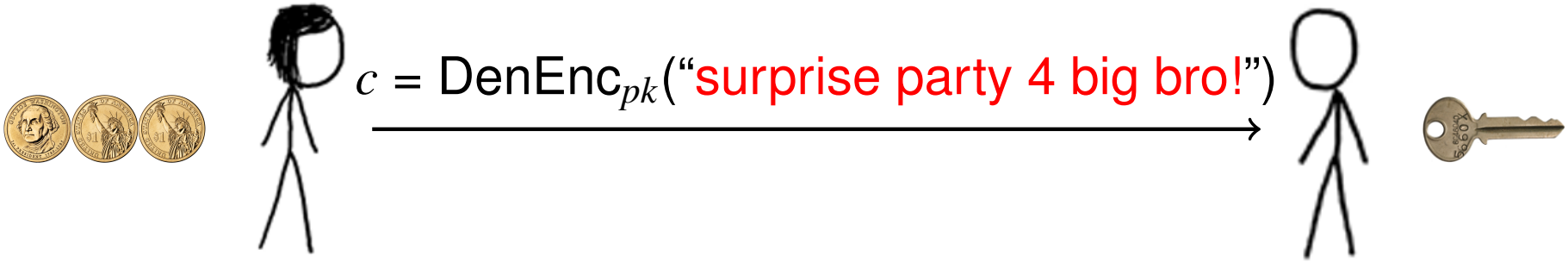
(Images courtesy xkcd.org)

Deniable Encryption



(Images courtesy xkcd.org)

Deniable Encryption

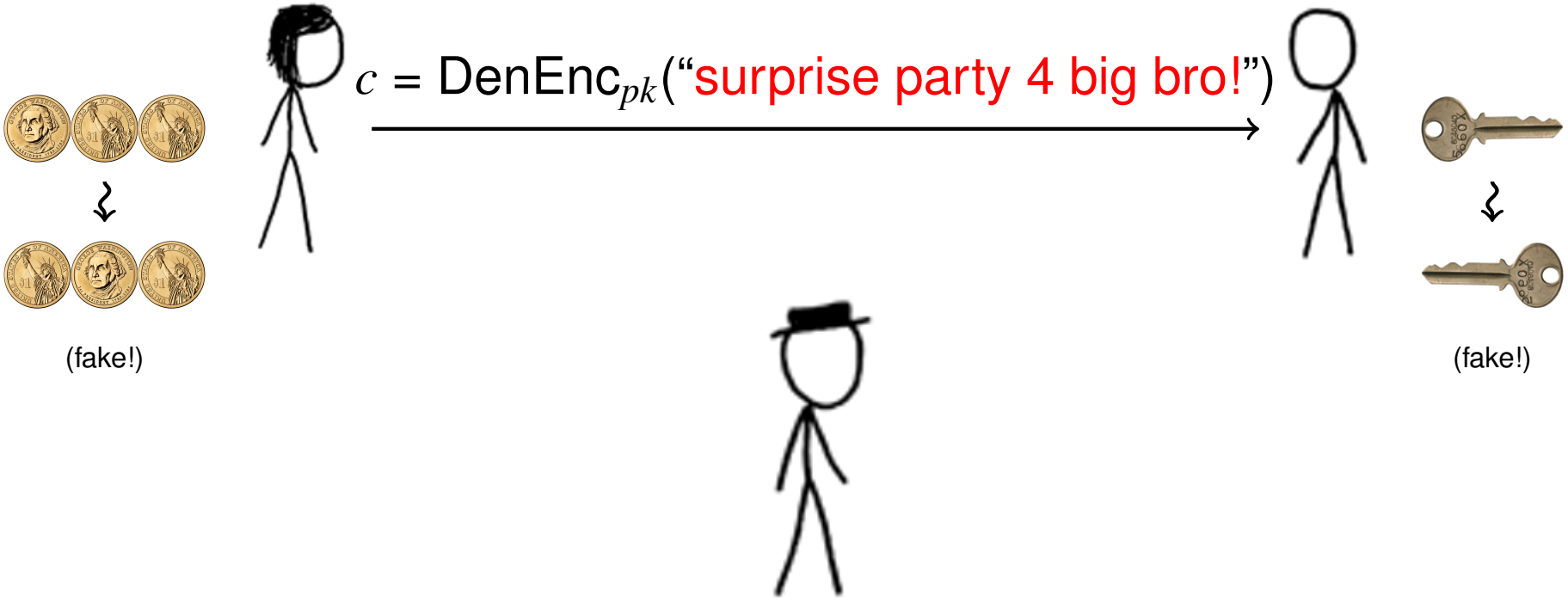


What We Want

1. Bob gets Alice's intended message, but . . .

(Images courtesy xkcd.org)

Deniable Encryption

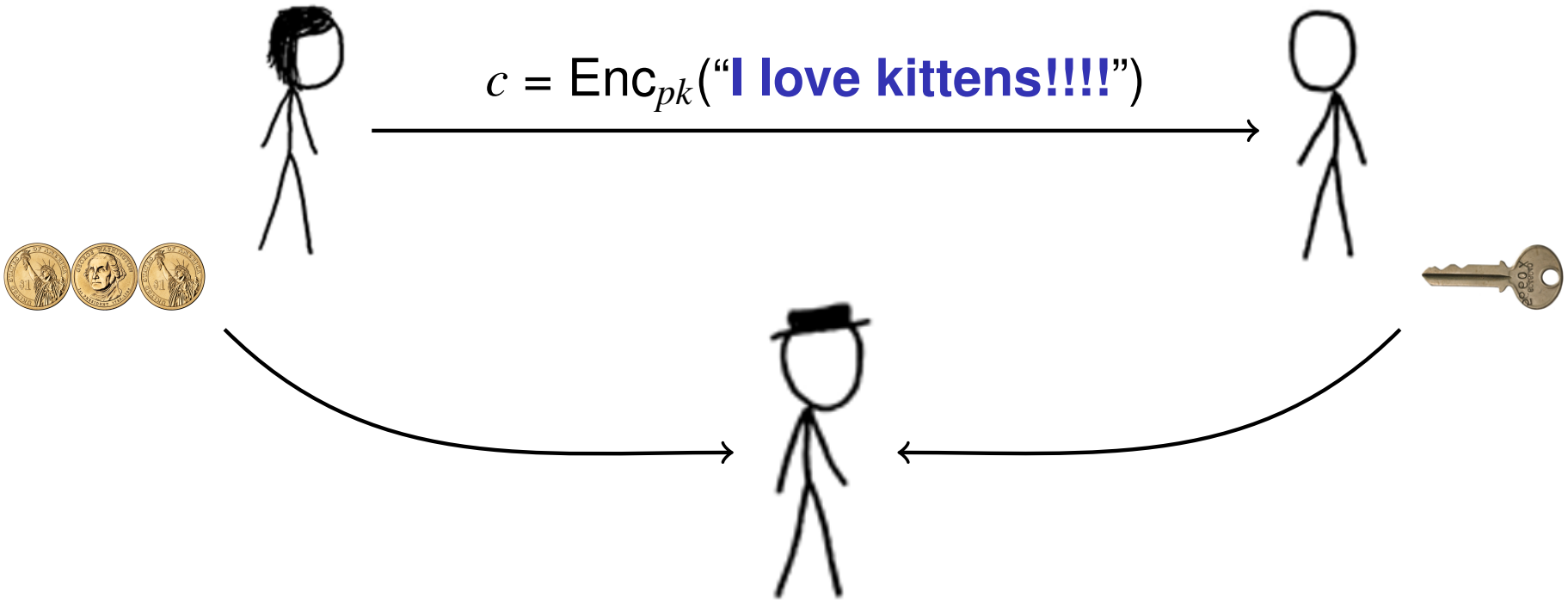


What We Want

1. Bob gets Alice's intended message, but . . .

(Images courtesy xkcd.org)

Deniable Encryption



What We Want

1. Bob gets Alice's intended message, but . . .
2. Fake coins & keys 'look as if' another message was encrypted!

(Images courtesy xkcd.org)

Applications of Deniability

1. Anti-coercion: ‘off the record’ communication (journalists, lawyers, whistle-blowers), 1984

Applications of Deniability

1. Anti-coercion: 'off the record' communication (journalists, lawyers, whistle-blowers), 1984

2. Voting: can reveal *any* candidate, so can't 'sell' vote (?)

Applications of Deniability

1. Anti-coercion: 'off the record' communication (journalists, lawyers, whistle-blowers), 1984

2. Voting: can reveal *any* candidate, so can't 'sell' vote (?)

3. Secure protocols tolerating *adaptive* break-ins [CFGN'96]

State of the Art

Theory [CanettiDworkNaorOstrovsky'97]

- Sender-deniable encryption scheme (under many standard assumps)
- Receiver-deniability by adding interaction & switching roles
- Bi-deniability by interaction w/ 3rd parties (one must remain uncoerced)

State of the Art

Theory [CanettiDworkNaorOstrovsky'97]

- Sender-deniable encryption scheme (under many standard assumps)
- Receiver-deniability by adding interaction & switching roles
- Bi-deniability by interaction w/ 3rd parties (one must remain uncoerced)

Practice: TrueCrypt, Rubberhose, ...

- Limited deniability: "*move along, no message here...*"

  Plausible for *storage*, but not so much for *communication*.

This Work

1. Bi-deniable encryption: sender & receiver *simultaneously* coercible

This Work

1. Bi-deniable encryption: sender & receiver *simultaneously* coercible
   - ⋆ A true public-key scheme: non-interactive, no 3rd parties
   - ⋆ Uses special properties of lattice-based TDFs and IBE [GPV'08]
   - ⋆ Has large keys . . . but this is inherent [Nielsen'02]

This Work

1. Bi-deniable encryption: sender & receiver *simultaneously* coercible
   - ⋆ A true public-key scheme: non-interactive, no 3rd parties
   - ⋆ Uses special properties of lattice-based TDFs and IBE [GPV'08]
   - ⋆ Has large keys . . . but this is inherent [Nielsen'02]

2. "Plan-ahead" bi-deniability with *short* keys
   - ⋆ Bounded number of alternative messages, decided in advance

Main Idea in a Nutshell

1. In the GPV'08 IBE, each ID has many possible secret keys sk_{ID}. Some (rare) sk_{ID}'s cause incorrect decryption — obliviously.

Main Idea in a Nutshell

1. In the GPV'08 IBE, each ID has many possible secret keys sk_{ID}.
   Some (rare) sk_{ID}'s cause incorrect decryption — obliviously.

2. Given msk and any ciphertext c encrypted to ID,
   can generate a 'fake' sk^*_{ID} that decrypts c to a random bit.

Main Idea in a Nutshell

1. In the GPV'08 IBE, each ID has many possible secret keys sk_{ID}.
   Some (rare) sk_{ID}'s cause incorrect decryption — obliviously.

2. Given msk and any ciphertext c encrypted to ID,
   can generate a 'fake' sk^*_{ID} that decrypts c to a random bit.

3. The 'fake' $sk^*_{ID} \approx_c$ 'true' sk_{ID}. (New analysis techniques here.)