Spam and Cybercrime

SMTP

- Simple Mail Transfer Protocol
  - Client connects to server on TCP port 25
  - Client sends commands to server
  - Server acks or notifies of error
- Security issues
  - Sender NOT authenticated
  - Message and headers transmitted in plain text
  - Message and header integrity NOT protected
  - Spoofing trivial to accomplish

- Example SMTP session

HELO mail.university.edu

MAIL FROM: president@whitehouse.gov

RCPT TO: chancellor@university.edu

DATA

From: president@whitehouse.gov

To: chancellor@university.edu

Date: April 1, 2010

Subject: Executive order

You are hereby ordered to increase the stipend of all TAs by $10,000 per year.

Sincerely,

The President of the United States

.

What is Email Spam?

- Email spam is often defined as unsolicited bulk email
  - Accounted for about 94% of all email sent
  - Spam costs businesses about $100 bill per year
  - Forbidden by all major ISPs
  - Considered “acceptable business practice” by US Direct Marketing Association (DMA)
- Spam arises from the combination of unsolicited and bulk

What is Email Spam?

- The US CAN-SPAM act (2004) regrettably protects commercial spam provided some requirements are satisfied, including:
  - Opt-out mechanism
  - Sender clearly identified and subject line not deceptive
  - Adult material labeled in subject line

Harvesting addresses

- Mailing lists and addresses are collected automatically by crawling the Web.
  - Post email address as john (dot) smith (at) example (dot) com
- Often buy and sell email lists from other spammers, advertising partners or criminal networks.
  - Give emails to only trusted parties and review web site's privacy policy before providing email address.

Sending Spam

- Most common technique is to hide the origin of email by simply spoofing the FROM field of the message. But the IP address of sender's SMTP server is also included in the email header, which can be revealed by further investigation.
- If SMTP server is configured as an open replay, the server can send email from any recipient to any destination. Today few mail servers allow this behavior.
- The open proxies can hide the true source and appear to recipient that the message comes from proxy. This provides users with the ability to browse the Internet anonymously but inherently insecure and malicious.
- Computers infected with malware are used to send spam

Web Mail

- Spammers can register an account with a free webmail service and use that account to send spam until the webmail provide detects this activity.
- To combat automated email account creation, most webmail services require users to solve a CAPTCHA (Completely Automated Public Turing test to tell computers and humans apart).
- Most of them are image recognition or distorted text.
- Some spammers copy the user provided solution to register.
- Some even employ low-paid workers to solve the CAPTCHA problem.
- CAPTCHA increases spammers' cost.

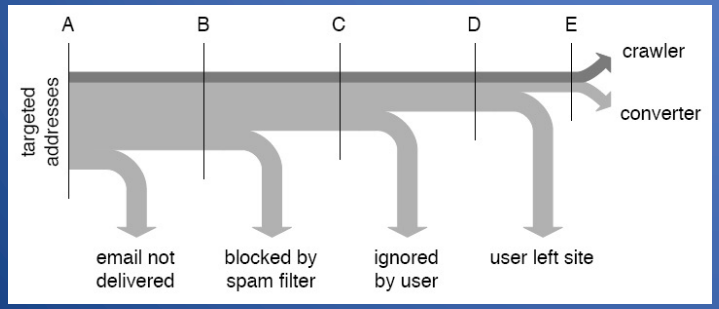
The Economics of Spam

- Spamming is profitable for spammers.
- Sending email incurs little expense on the sender because nearly all of the operational costs associated with storing large volumes of information are forced on the unwilling recipients.
- The total return is generally greater than the expenses.

A princess in Nigeria wants to send me money!

Spam Conversion

- Conversion rate is the percentage of spam recipients who follow through and perform some desired action that results in the spammer receiving money
- Empirical study [Kanich+ 2008]
  - Parasitic infiltration into botnet launching spam campaign for "Canadian drugs"
  - 28 conversions, yielding $3K, from 300M spam messages over 26 days



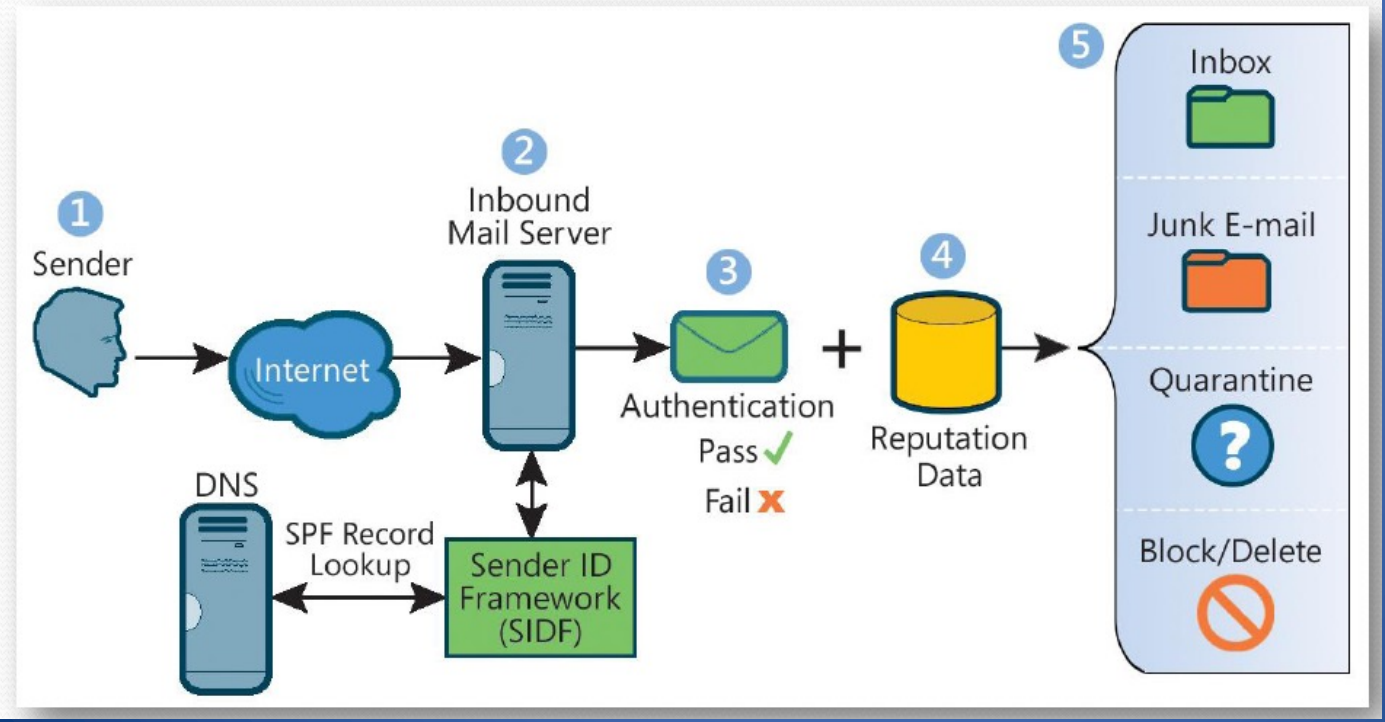
Yes, Honey, you ***could*** benefit from that drug.

Blacklisting and Greylisting

- Blacklisting
  - Real-time database of IP addresses of verified spam sources
  - Eliminates about 10% of spam before transmission takes place
  - Formal listing and delisting procedures
  - More than 600M email users protected by blacklisting
- Greylisting
  - Spam servers typically do not resend messages after transmission errors
  - Maintain database of trusted servers
  - Respond with “Busy, please retry” to SMPT connection requests from servers not in database
  - Server added to database if reestablishes connection
  - Currently effective although simple to circumvent

Sender ID and Sender Policy Framework

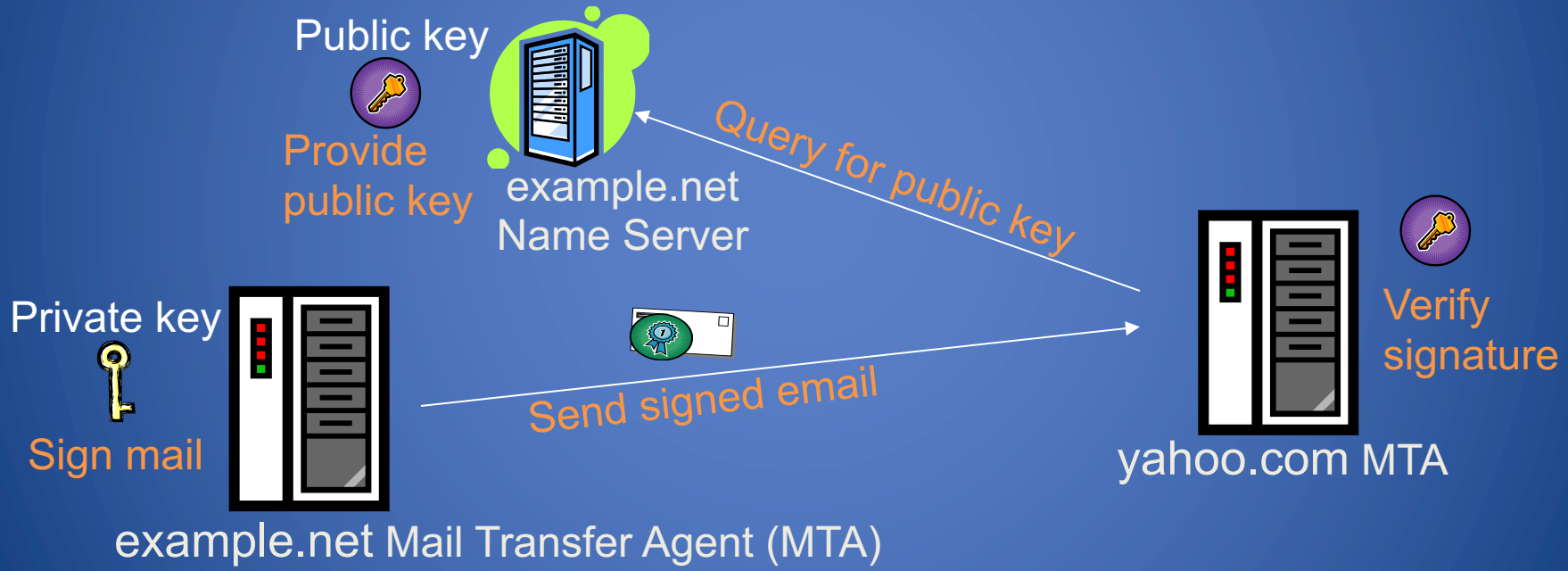
- Store DNS records about severs authorized to send mail for a given domain
- Look up domain in From header to find IP address of authorized mail server



Source: Microsoft

DomainKeys Identified Mail (DKIM)

- Sender's mail server signs email to authenticate domain
- Public key of server available in DNS record
- To be used in conjunction with other spam filtering methods



DomainKey-Signature: a=rsa-sha1; s=mail; d=example.net; c=simple; q=dns; b=Fg…5J

Authentication-Results: example.net from=bob@example.net; domainkeys=pass;

Sender Policy Framework (SPF) vs. DKIM

SPF

- The IP address of the MTAs authorized to send mail for a domain are stored in a DNS text record for that domain
- The receiving MTA checks that the IP of the sending MTA is in the list of authorized IP address for the sender's domain.
- Simple implementation
- Message integrity not protected
- Mail forwarding not supported
- Vulnerable to DNS cache poisoning
- Vulnerable to IP source spoofing

DKIM

- Sending MTA authentication
- Object based
- Cryptographic assurance
- Protection of message integrity
- Supports mail forwarding
- Vulnerable to DNS cache poisoning

Cybercrime

- Symantec's definition:
  - Cybercrime is any crime that is committed using a computer, network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations.
- Enablers of cybercrime
  - Software vulnerabilities
  - Online shopping and access to financial accounts
  - Countries with lax or corrupt law enforcement

Credit Cards

- Credit card information
  - Supposed to be kept secret
  - Shared with multiple merchants
  - Transmitted often insecurely
  - Low entropy of the credit card number (first four digits denote financial institution)
- Advantage
  - Simple scheme for users, banks, and merchants
- Disadvantage
  - Fraud easy to commit
- Tradeoff
  - No security measures to facilitate use
  - Private customers and merchants held harmless
  - Transaction fee covers bank fraud losses

Common Credit Card Frauds

- Buy popular goods and resell them
  - Needs package delivery address
  - Requires resale business
  - Often goods reshipped abroad
- Buy financial instruments
  - Traveler's checks
  - Gift cards
  - E-gold
  - Additional conversion needed to avoid revocation
- Buy cash equivalents
  - Western Union money transfers
  - Foreign currency

Defending Against Credit Card Fraud

- One-time credit card numbers
  - Available from several issuers (e.g., AmEx, Citibank)
  - Does not work for subscription plans
  - Time consuming for users
  - Cumbersome to obtain refunds
  - Worthwhile for high-value transactions or untrusted merchants
- Monitoring transactions
  - Email or text message for each transaction
  - Continuous annoyance to catch a rare event
- Password enabled transactions
  - Similar to PIN for ATM cards
  - Difficult to share password only with the bank and communicate verification outcome to merchant (three-party protocol)

Bank Accounts

- Account information
  - Supposed to be kept secret
  - Shared with merchants, customers and friends
  - Same account number for deposits and withdrawals
- Typical bank transactions
  - Check
  - ATM
  - Wire transfer
- Banking in the US
  - Account title
  - Taxpayer ID Number (TIN)
  - Checks can be generated by customers or third parties
  - Signature not verified in practice for amounts below $30K
  - Automated Clearing House (ACH), regulated by Federal Reserve, supports interbank transfers, direct deposits and direct debits
  - ACH allows one to initiate from account A an inbound transfer into A from any account B with same TIN as A

Common Bank Frauds

- Forged checks
  - Create checks with magnetic ink printers
  - Cash with fake ID
  - Low amounts typically not scrutinized
- Wire transfer
  - Send fax to bank to order wire transfer
  - Most effective if money wired abroad
- Account creation
  - Create account A impersonating owner of account B
  - ACH transfer from B to A
  - Cash with ATM or wire transfer

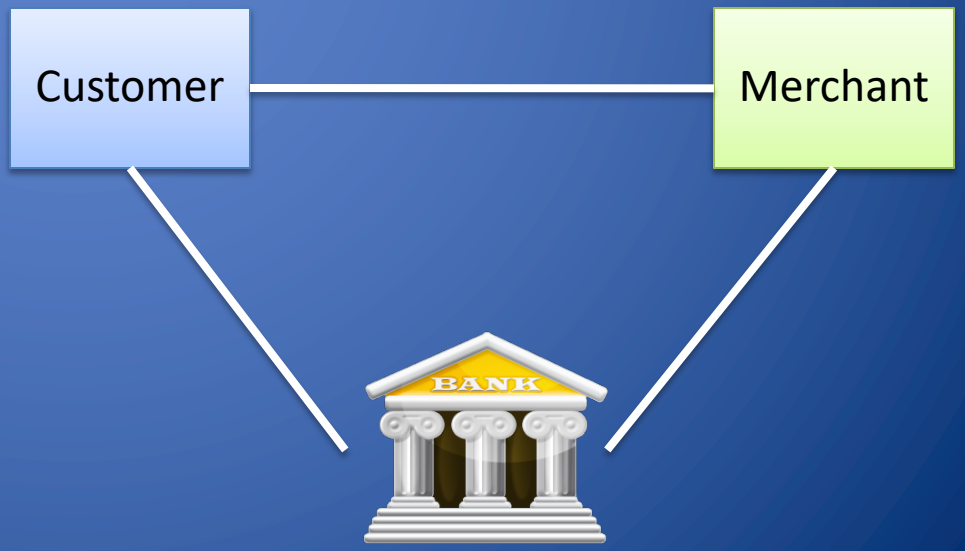
Defending Against Bank Fraud

- Multi-factor authentication
  - Hardware token generating one-time codes
  - Personal images and sentences to defend against phishing
  - Code sent by email/sms to registered address to authorize debit transactions
- Account ownership verification
  - Linking accounts for ACH transfers requires knowledge of to small deposits to the account
- Restrictions on accounts
  - E.g., only credit transaction accepted
- Monitoring bank transactions
  - Email/text message after each transactions
- No online banking
  - Limited bank liability for online frauds

Payment Systems

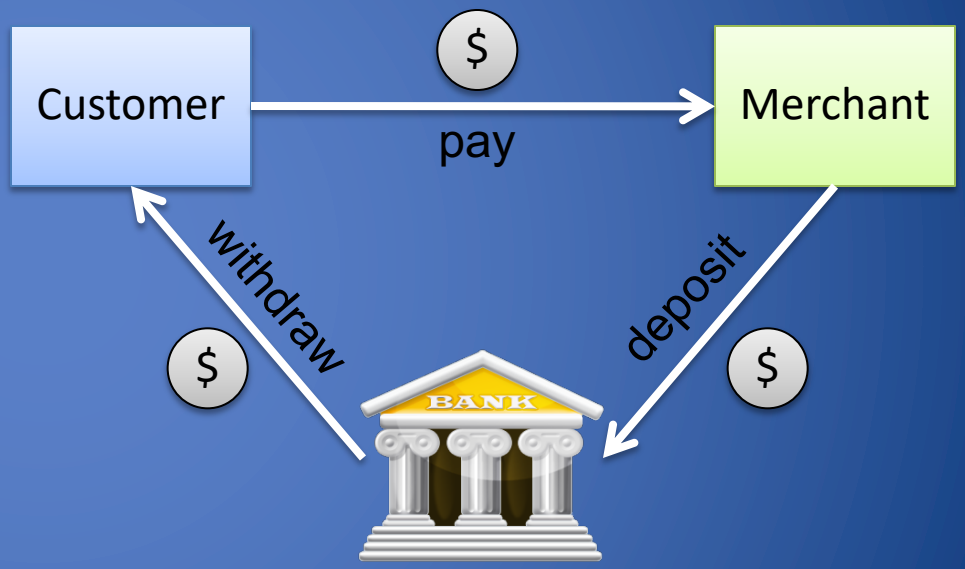
Electronic Payment Schemes

- Schemes for electronic payment are multi-party protocols
- Payment instrument modeled by electronic coin that has a fixed value and can be exchanged with a traditional monetary instrument
- Parties include:
  - Payer (customer)
  - Payee (merchant)
  - Bank



Transactions

- Transactions in an electronic payment scheme typically include:
  - Withdrawal of coins by customer from the bank
  - Payment of coins by customer to merchant
  - Deposit of coins by merchant into bank



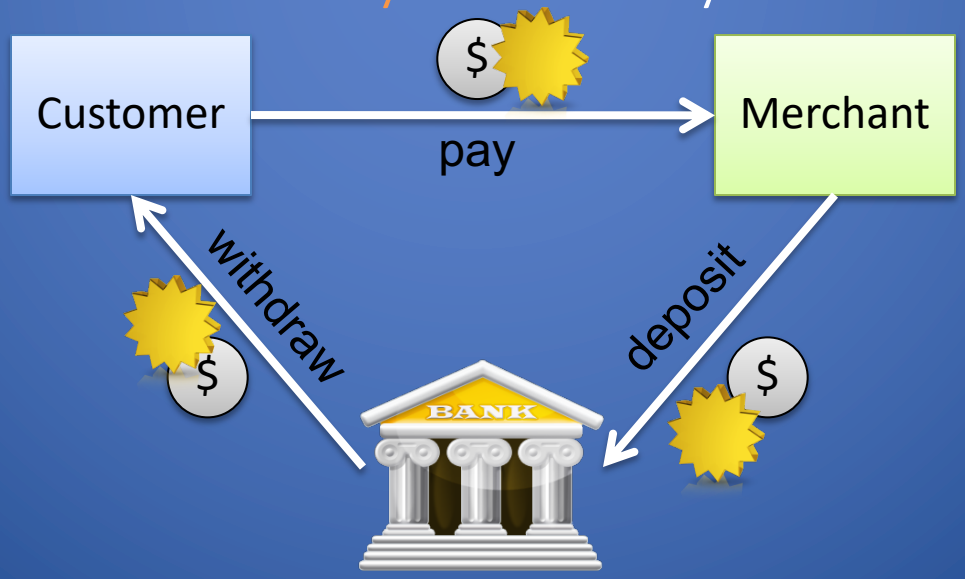
- Online scheme:
  - The bank participates in the payment transaction
- Offline scheme
  - The bank does not participate in the payment transaction

Goals

- Integrity
  - Coins cannot be forged
  - Legitimate transactions are honored
- Accountability
  - Transactions cannot be later denied
  - Disputes can be efficiently settled
- Privacy
  - The identity of some parties is not revealed to other parties
  - Coins cannot be traced to the payer and/or payee (digital cash)

Payment with Digital Signatures

- Coins are random identifiers digitally signed by the bank at the time of withdrawal
- The merchant verifies the signature by the bank
- The bank honors deposit of valid coins
- Security and privacy issues:
  - Customer can copy coin and double spend
  - The bank learns about every transaction by customer and merchant



Private Payment Scheme

- A blind signature allows the signed to sign a message without knowing the message itself
- Basic digital cash scheme:
  - The bank does a blind signature on the coins withdrawn by the customer
  - The merchant verifies the signature and deposits the coins
  - The bank cannot link the coins to the customer

Fair Electronic Exchange

- Objective:
  - Either both parties obtain each other's items or none of them do.

- Types of Implementations:
  - Fair Contract Signing
  - Fair Certified E-Mail
  - Online payment systems

Contract Signing

C = Contract

Alice

$Sig_A(C)$ →

← $Sig_B(C)$

Bob

[redacted]

Fair Contract Signing

C = Contract

Alice

$Sig_A(C , Z)$ →

← $Sig_B(C , Z)$

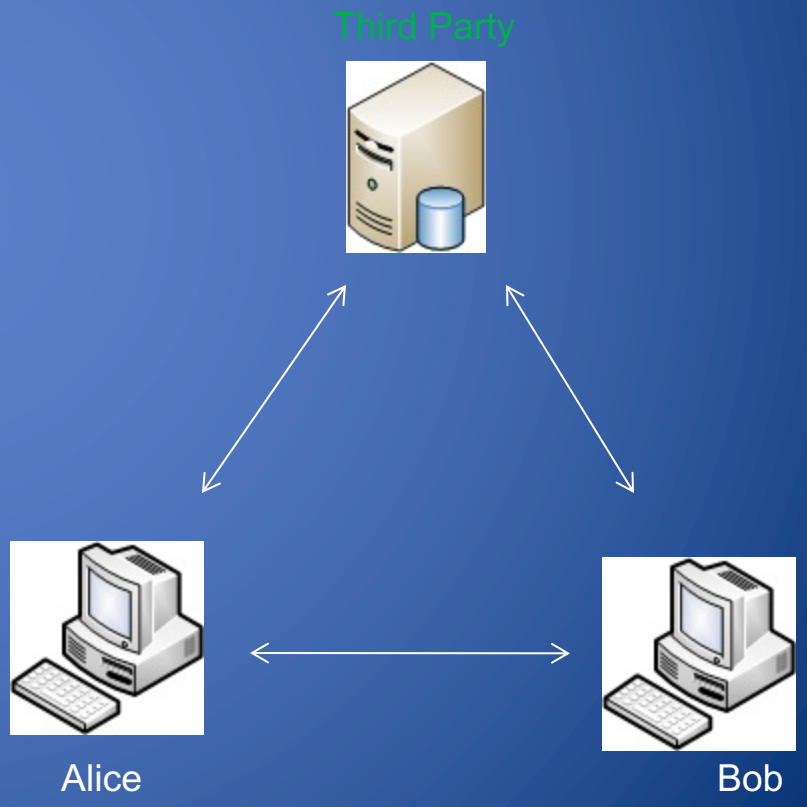
Bob

Z Z

Z

Trusted Third Party

- An entity that provides justice by processing Z
  - Trusted by everybody
- Types:
  - Online Third Parties
    - Participate in every transaction
    - Easy to implement
    - Resource hungry
  - Offline Third Parties
    - Participates only when cheating occurs
    - Efficient

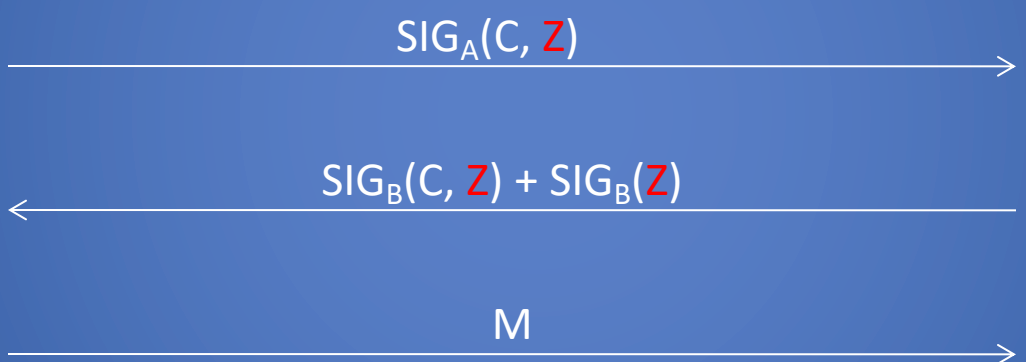


Micali's Protocol

Normal Execution

Alice **Bob**

Chooses random M
and computes
$Z = E_{TP}(A, B, M)$



Bob re-computes Z
from M received.

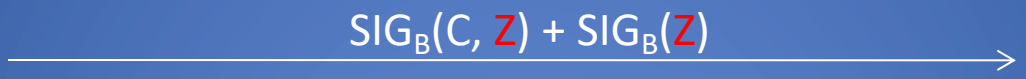
If(match)
contract complete!
Else
contact TP

Legend:
A: Alice's Identity
B: Bob's Identity
M: Secret known only to Alice
E_{TP} (*): Encryption using TP's Public Key

Micali's Protocol

Resolution Phase

Bob **Third Party**



1. Decrypt Z using Private Key

2. Verify the signatures for their validity.

If(Valid)
    Send M to Bob
Else
    No Action

References

- The electronic cash scheme presented in this lecture is based on the work by David Chaum http://www.chaum.com/
- D. Chaum, A. Fiat, and M. Naor. *Untraceable Electronic Cash*, in Proc. CRYPTO 1988. http://citeseer.ist.psu.edu/421212.html
- S. Goldwasser and M. Bellare. *Lecture Notes on Cryptography* [Section 12.5] http://www-cse.ucsd.edu/users/mihir/papers/gb.html