Lecture 3. Electronic Commerce Security
전자상거래 보안

2008. 10. 17.

Prof. Byoungcheon Lee
sultan (at) joongbu . ac . kr

Dept. of Information Security
Joongbu University

Contents

1. Electronic Commerce
2. Electronic Payment
3. Secure Electronic Transaction (SET)
4. Electronic Auction
5. Electronic Voting

1. Electronic Commerce

E-Commerce and E-Business

- **Electronic commerce** (**e-commerce, EC**) describes the buying, selling, transferring or exchanging of products, services or information via computer networks, including the Internet.

- **E-business** is a broader definition of EC that includes not just the buying and selling of goods and services, but also
  - Servicing customers
  - Collaborating with business partners
  - Conducting electronic transactions within an organization

Pure EC vs. Partial EC

- **Pure EC vs. Partial EC: based on the degree of digitization of product, process, delivery agent**
  - ✓ **The product can be physical or digital**
  - ✓ **The process can be physical or digital**
  - ✓ **The delivery agent can be physical or digital**

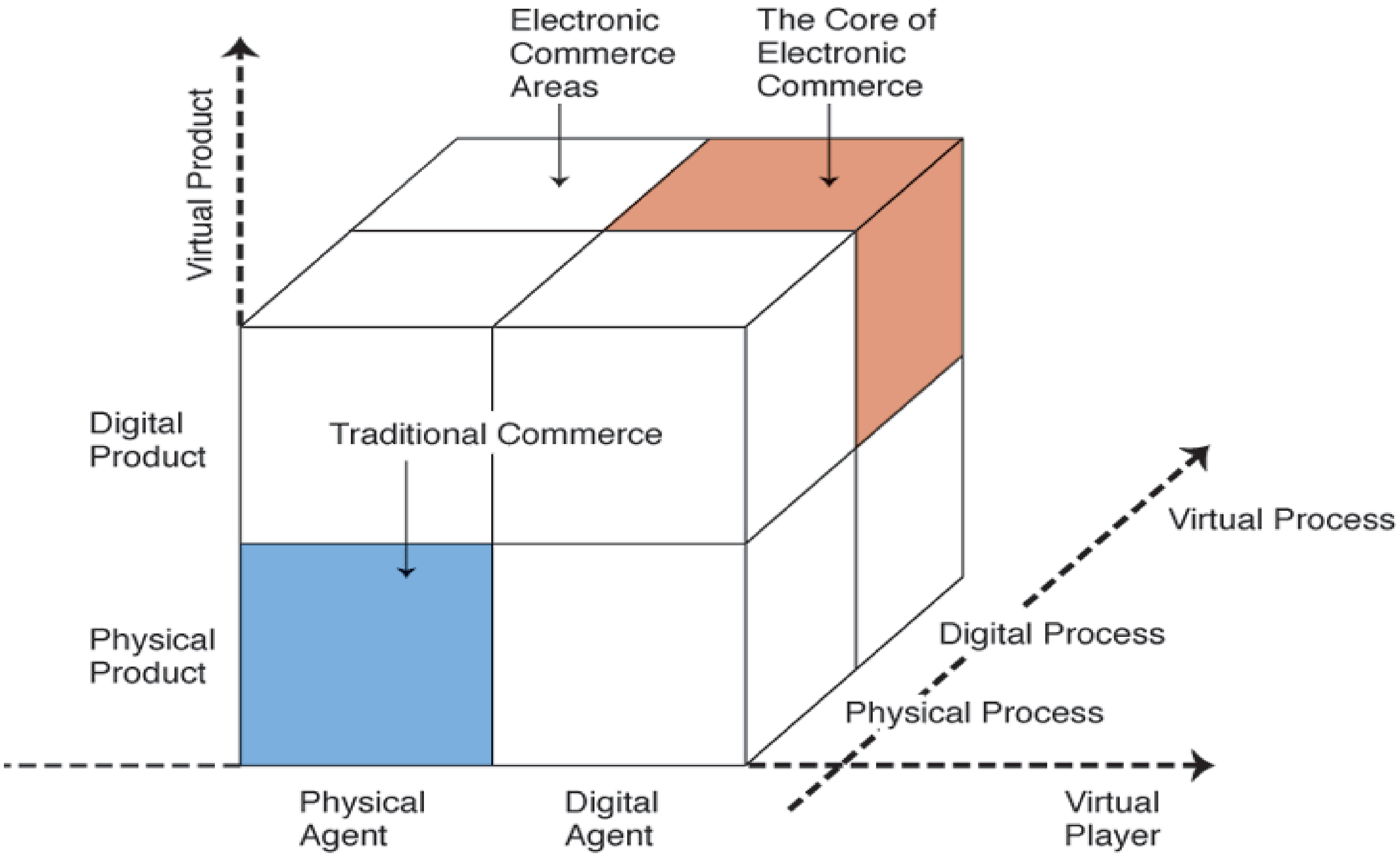
- **Brick-and-mortar organizations are purely physical organizations.**

- **Click-and-mortar organizations are those that conduct some e-commerce activities, yet their business is primarily done in the physical world. i.e. *partial EC***

- **Virtual organizations are companies that are engaged only in EC. i.e. *pure EC***

Dimensions of EC

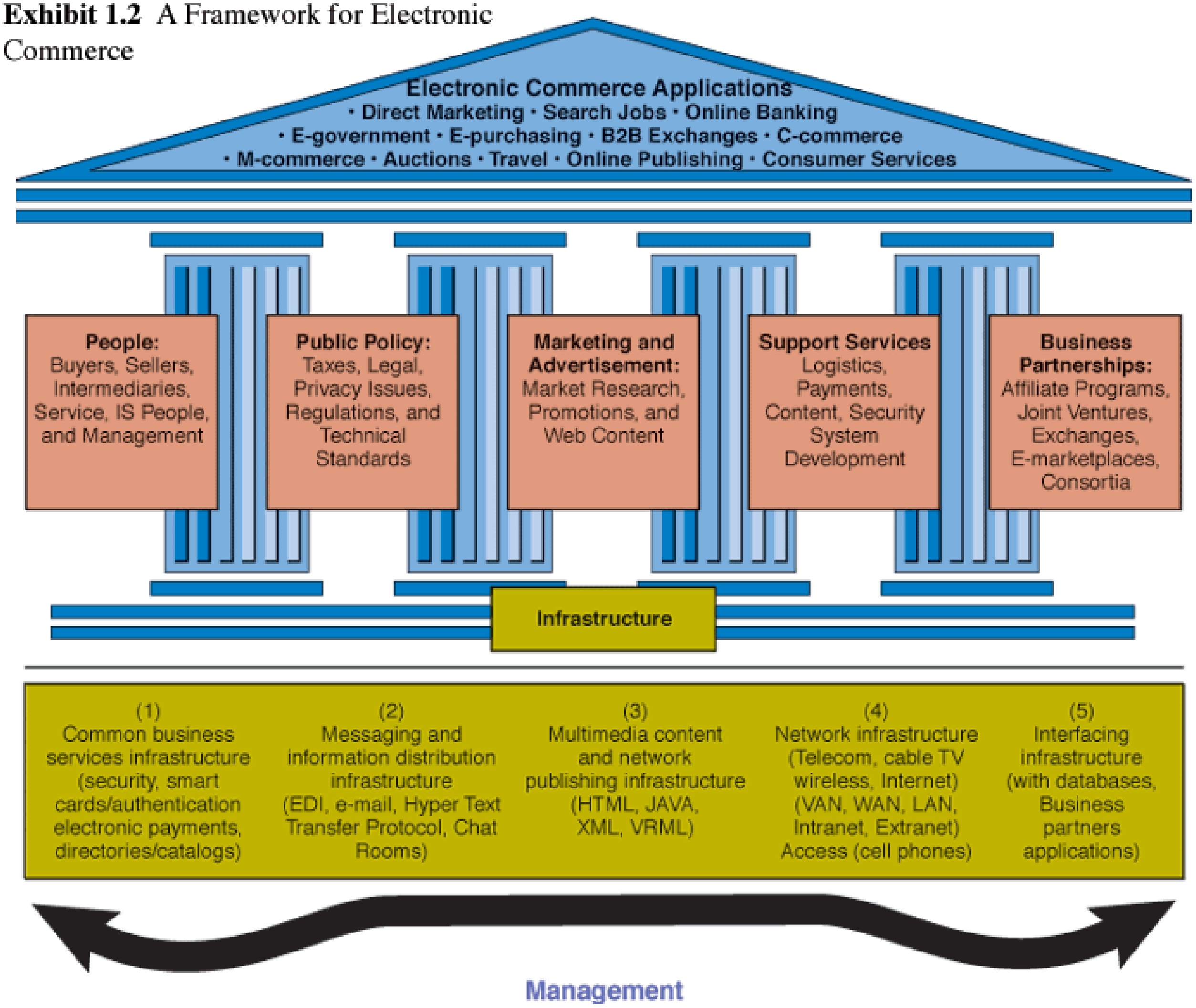
Exhibit 1-1 The Dimensions of Electronic Commerce



Source: Choi et al. (1997), p. 18.

A Framework for EC

Exhibit 1.2 A Framework for Electronic Commerce



Electronic Commerce Applications

• Direct Marketing • Search Jobs • Online Banking

• E-government • E-purchasing • B2B Exchanges • C-commerce

• M-commerce • Auctions • Travel • Online Publishing • Consumer Services

People: Buyers, Sellers, Intermediaries, Service, IS People, and Management

Public Policy: Taxes, Legal, Privacy Issues, Regulations, and Technical Standards

Marketing and Advertisement: Market Research, Promotions, and Web Content

Support Services Logistics, Payments, Content, Security System Development

Business Partnerships: Affiliate Programs, Joint Ventures, Exchanges, E-marketplaces, Consortia

Infrastructure

(1) Common business services infrastructure (security, smart cards/authentication electronic payments, directories/catalogs)

(2) Messaging and information distribution infrastructure (EDI, e-mail, Hyper Text Transfer Protocol, Chat Rooms)

(3) Multimedia content and network publishing infrastructure (HTML, JAVA, XML, VRML)

(4) Network infrastructure (Telecom, cable TV wireless, Internet) (VAN, WAN, LAN, Intranet, Extranet) Access (cell phones)

(5) Interfacing infrastructure (with databases, Business partners applications)

Management

Brief History of EC

- **Electronic Fund Transfer (EFT) – early 1970s**
  - **Limited to large corporations, financial institutions**

- **Electronic data interchange (EDI) — electronic transfer of documents:**
  - **Purchase orders**
  - **Invoices**
  - **E-payments between firms doing business**

- **Inter-Organizational systems (IOS)**
  - **Stock trading**
  - **Travel reservation systems**

- **Internet became more commercialized in the early 1990s**
  - **Almost all medium and large-sized organizations in the world now have a Web site**
  - **Most large corporations have comprehensive portals**

Categories of E-Commerce

- Business-to-consumers (B2C)
- Business-to-business (B2B)
- Consumer-to-consumer (C2C)
- Business-to-employee (B2E)
- Government-to-Business (G2B) – E-Government
- Government-to-Customer (G2C) – E-Government
- Mobile Commerce (M-Commerce)

Benefits of E-Commerce

- **Benefits to organizations**
  - Makes national and international markets more accessible
  - Lowering costs of processing, distributing, and retrieving information
  - Allows reduced inventories and overhead by facilitating pull-type supply chain management
  - The pull-type processing allows for customization of products and services which provides competitive advantage to its implementers
  - Reduces the time between the outlay of capital and the receipt of products and services
  - Supports business processes reengineering (BPR) efforts
  - Lowers telecommunications cost - the Internet is much cheaper than value added networks (VANs)

Benefits of E-Commerce

❖ **Benefits to customers**

- Enables consumers to shop or do other transactions 24 hours a day, all year round from almost any location
- Provides consumers with more choices
- Provides consumers with less expensive products and services by allowing them to shop in many places and conduct quick comparisons
- Allows quick delivery of products and services (in some cases) especially with digitized products
- Consumers can receive relevant and detailed information in seconds, rather than in days or weeks
- Makes it possible to participate in virtual auctions
- Allows consumers to interact with other consumers in electronic communities and exchange ideas as well as compare experiences
- Facilitates competition, which results in substantial discounts

Benefits of E-Commerce

❖ **Benefits to Society**

- Enables more individuals to work at home, and to do less traveling for shopping, resulting in less traffic on the roads, and lower air pollution
- Allows some merchandise to be sold at lower prices, benefiting less affluent people
- Enables people in Third World countries and rural areas to enjoy products and services which otherwise are not available to them
- Facilitates delivery of public services at a reduced cost, increases effectiveness, and/or improves quality

Limitations of E-Commerce

❖ **Technological Limitations**

- Lack of universally accepted security standards
- Insufficient telecommunications bandwidth
- Expensive accessibility

❖ **Non-technological Limitations**

- Perception that EC is insecure
- Unresolved legal issues
- Lacks a critical mass of sellers and buyers

B2C E-Commerce

- Electronic Storefront has its own URL at which buyers can place orders.
- Electronic Malls (Cybermall or e-mall) is a collection of individual shops under one Internet address.
- Cyberbanking (electronic banking) conducting various banking activities outside of a physical banking location.
- Online Securities Trading uses computers to trade stocks, bonds and other financial instruments.
- Online Job Market advertises available positions, accept resumes and takes applications via the Internet.
- Travel Services plan, explore and arrange almost any trip economically over the Internet.
- Real Estate view, sort and organize properties according to your preferences and decision criteria.
- Really Simple Syndication (RSS) information that you request, called a feed, comes to you daily through a piece of software called a newsreader.

B2B E-Commerce

- Sell-side marketplaces are where organizations attempt to sell their products or services to other organizations electronically from their own private e-marketplace.
- Buy-side marketplaces are where organizations attempt to buy needed products or services from other organizations electronically.
- E-Procurement is using electronic support to purchase goods and materials, sourcing, negotiating with suppliers, paying for goods and making delivery arrangements.
- Group purchasing is when the orders of many buyers are combined so that they constitute a large volume.
- Airways business example
  - Other airways
  - Travel agents
  - Etc…

2. Electronic Payment

Electronic Payment

- Electronic payment systems enable you to pay for goods and services electronically.
  - Electronic checks (e-checks) are similar to paper checks and are used mostly in B2B.
  - Electronic credit cards allow customers to charge online payments to their credit card account.
  - Purchasing cards are the B2B equivalent of electronic credit cards and are typically used for unplanned B2B purchases.
  - Electronic cash: Stored-value money cards allow you to store a fixed amount of prepaid money and then spend it as necessary.

- Electronic payment is an indispensable technology for Pure EC
  - Also a good application of crypto technology

Electronic Payment

- **How to protect payment information over the network?**
  - **Secure socket layer (SSL) — protocol that utilizes standard certificates for authentication and data encryption to ensure privacy or confidentiality**
  - **Transport Layer Security (TLS) — as of 1996, another name for the Secure Socket Layer protocol**
  - **Secure Electronic Transaction (SET) — a protocol designed to provide secure online credit card transactions for both consumers and merchants; developed jointly by Netscape, Visa, MasterCard, and others**

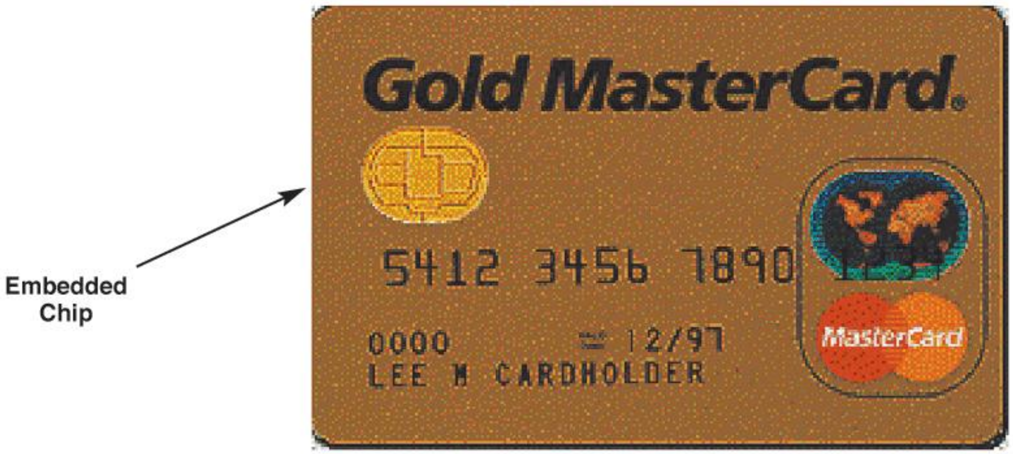
Electronic Payment

- **Electronic wallets (e-wallets) — a software component in which a user stores credit card numbers and other personal information; when shopping online; the user simply clicks the e-wallet to automatically fill in information needed to make a purchase**
  - **One-click shopping — saving your order information on retailer's Web server**
  - **E-wallet — software downloaded to cardholder's desktop that stores same information and allows one-click-like shopping**

Electronic Payment

- **Smart card—an electronic card containing an embedded microchip that enables predefined operations or the addition, deletion, or manipulation of information on the card**
  - **Contact card**
  - **Contactless card**

Exhibit 10.6 Smart Card Image



Classification of Electronic Payment

- **Electronic cash system: Electronic version of real world cash, Don’t need any broker in transaction**
  - ✓ **Network type: Ecash, Netcash, Millicent, PayMe, etc.**
  - ✓ **IC card type: Mondex, Visa Cash, PC pay, etc**

- **Payment broker system: A trusted broker mediates a payment transaction**
  - ✓ **Credit card system: SET, First Virtual (FV)**
  - ✓ **Electronic cheque system: NetCheque, Echeck**

Electronic Cash

- A digital data with monetary value (signed by bank)
  - (hidden) user information, user account, value
- "Digital Cash", "Cyber Cash", "Electronic Money", "Virtual Currency"

- Classification of electronic cash systems
  - IC card type / Network type cash
  - Online / Offline cash
  - Closed loop / Open loop cash
  - Pay in advance / Pay later

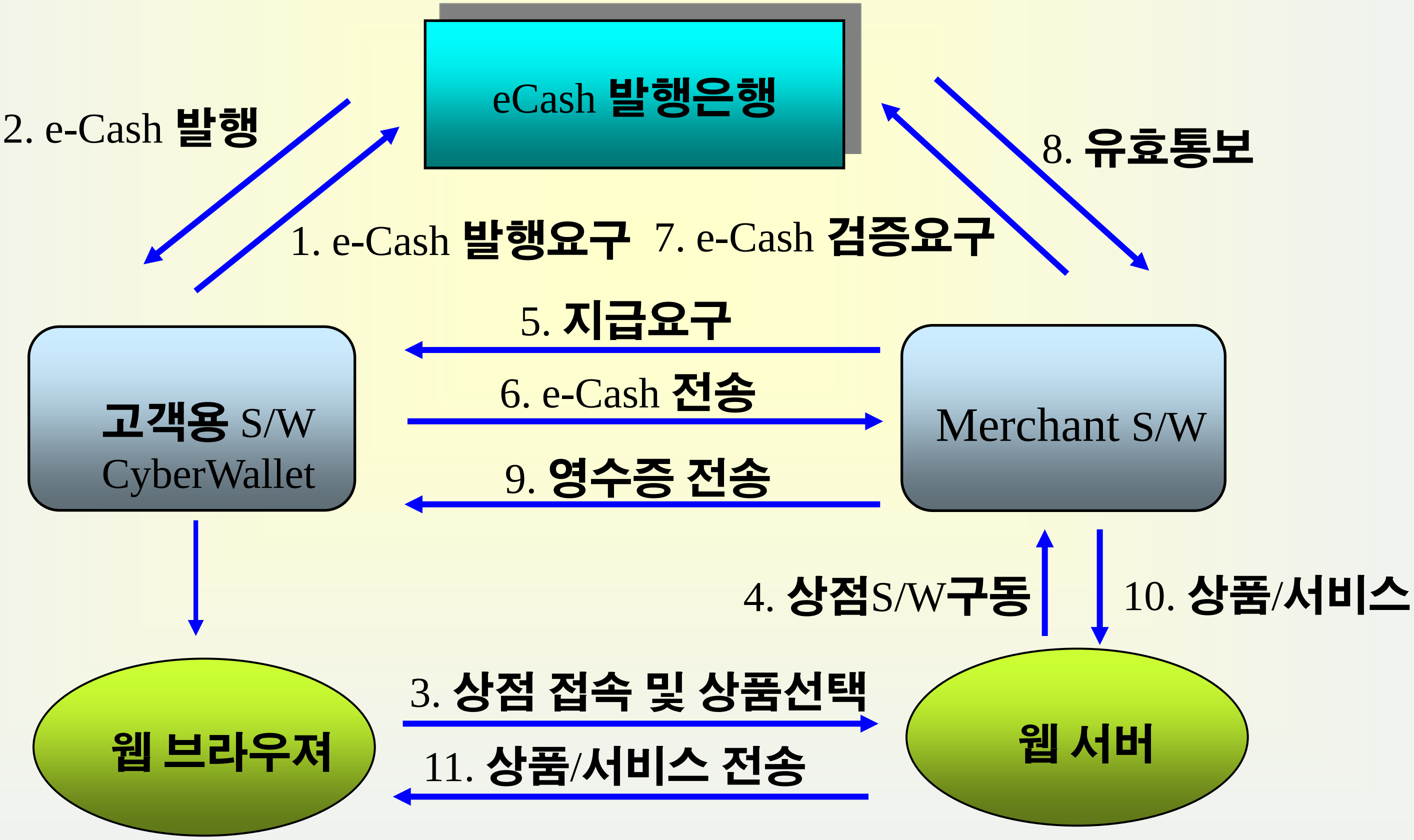
- Major electronic cash system
  - Network type: Ecash, Netcash, Millicent, PayMe, etc.
  - IC card type: Mondex, Visa Cash, PC pay, etc

Requirement of Electronic Cash System

- Security: against any forgery
- Privacy
  - Untraceability: user of a payment cannot be traced
  - Unlinkability: cannot link two payments
- Unreusability: prevent double spending
  - Detecting after double spending
  - Detecting before double spending occurs
- Offline payment: don’t need online communication with bank during payment
- Transferability: transferable to other user (not payment)
- Divisibility: divide and pay
- Anonymity revocation of illegal users

Ecash System

- Electronic cash using blind signature technology (RSA-based)
- Developed by D. Chaum in DigiCash (http://www.digicash.com/)
- Provide perfect anonymity

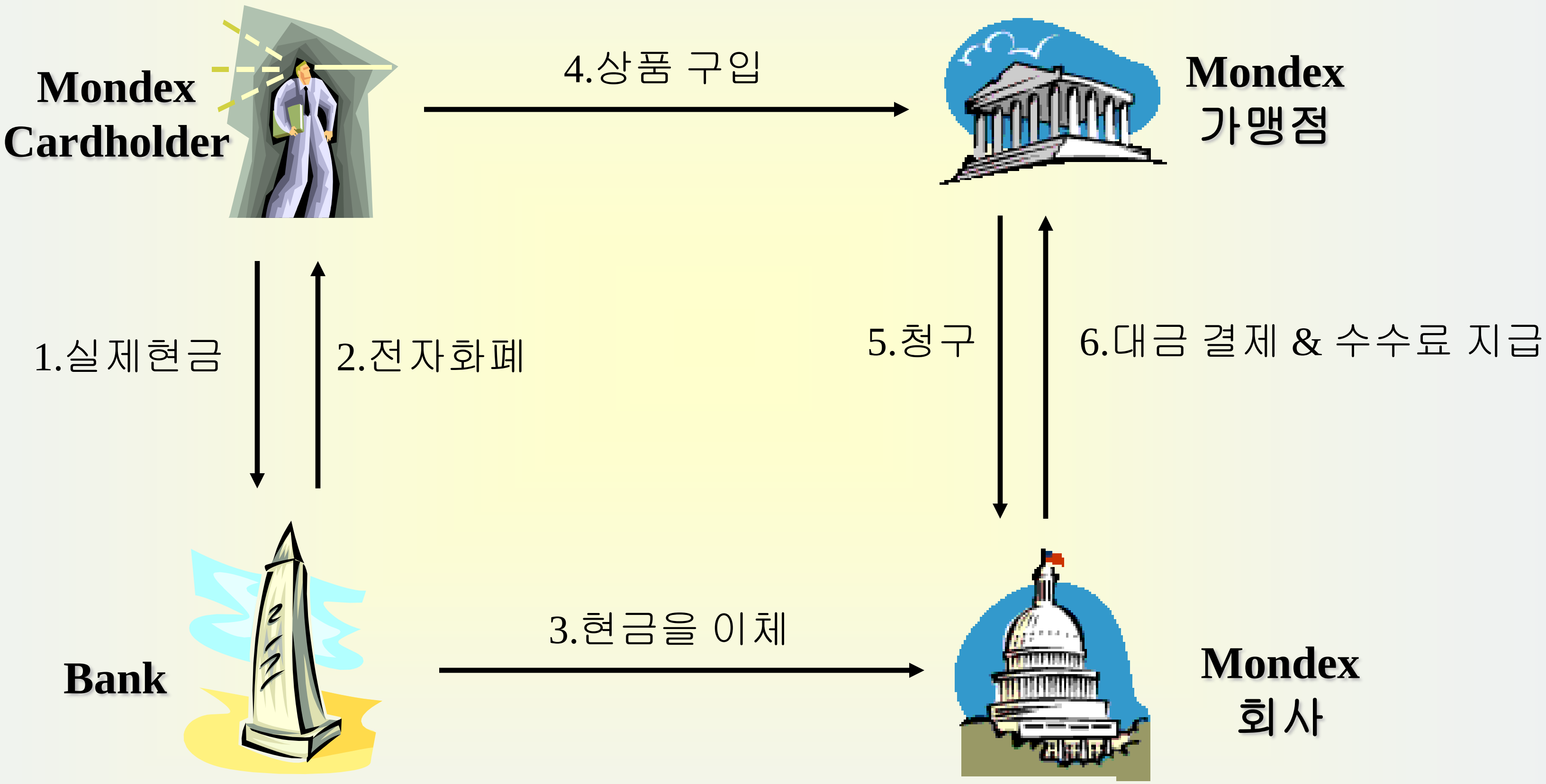


Mondex

- Smart card-based electronic cash system
- Offline cash
- COS(Chip Operating System): MULTOS (Multi-Application Operating System)

- System configuration
  - Mondex Wallet
  - Mondex Balance Reader
  - Mondex Telephone
  - Mondex Card

Mondex



Mondex Cardholder

4.상품 구입

Mondex 가맹점

1.실제현금

2.전자화폐

5.청구

6.대금 결제 & 수수료 지급

Bank

3.현금을 이체

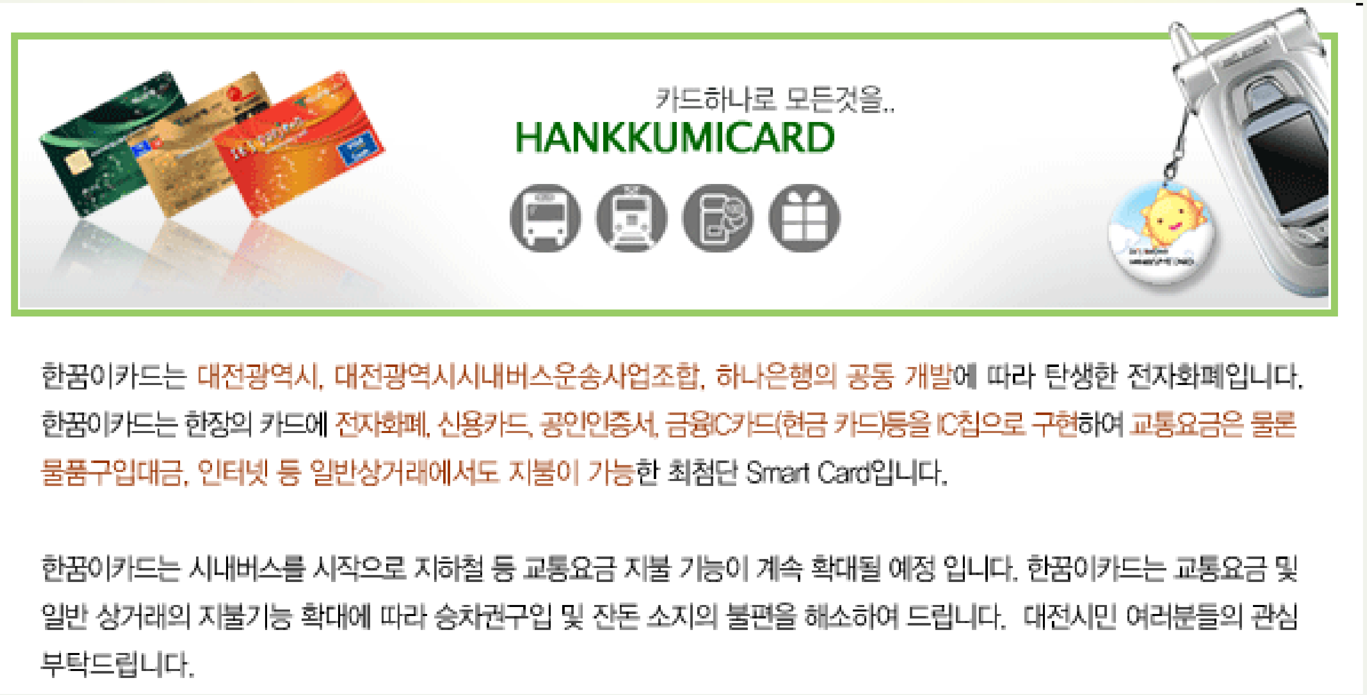
Mondex 회사

Comparison of Electronic Cash Systems

제품	보안 메카니즘	s/w 요구	h/w 요구	익명성	양도성
Mondex	마이크로 칩	X	O	strong	O
CyberCoin	RSA, DES	O	X	strong	X
PC Pay	h/w - based	O	O	strong	X
ecash	RSA	O	X	strong	X
PayMe	대칭&비대칭 키 암호	O	X	Resonably	X
NetCash	kerberos 인증	O	X	low	X
Visa Cash	마이크로 칩	O	O	O	X
Millicent	소액거래	O	X	Resonably	X
EIPaN	마이크로 칩	X	O	strong	X
NetFare	card & PIN number	X	O	strong	X

Electronic Cash Systems in Korea

❖ K-Cash:	http://www.kcash.or.kr/
❖ iCash:	http://www.icash.co.kr/
❖ Mybi:	http://www.mybi.co.kr/
❖ Visa Cash:	http://www.visacash.co.kr/



한꿈이카드는 대전광역시, 대전광역시시내버스운송사업조합, 하나은행의 공동 개발에 따라 탄생한 전자화폐입니다. 한꿈이카드는 한장의 카드에 전자화폐, 신용카드, 공인인증서, 금융IC카드(현금 카드)등을 IC칩으로 구현하여 교통요금은 물론 물품구입대금, 인터넷 등 일반상거래에서도 지불이 가능한 최첨단 Smart Card입니다.

한꿈이카드는 시내버스를 시작으로 지하철 등 교통요금 지불 기능이 계속 확대될 예정 입니다. 한꿈이카드는 교통요금 및 일반 상거래의 지불기능 확대에 따라 승차권구입 및 잔돈 소지의 불편을 해소하여 드립니다. 대전시민 여러분들의 관심 부탁드립니다.

3. Secure Electronic Transaction (SET)

Paying with Credit Card on the Internet

- **Problem: communicate credit card and purchasing data securely to gain consumer trust**
  - **Authentication of buyer and merchant**
  - **Confidential transmissions**

- SSL (Secure Socket Layer)
- TLS (Transport Layer Security)
  - IETF version of SSL

Communication Security

- *i* KP (Internet Keyed Payment, IBM)
- SEPP (Secure Encryption Payment Protocol)
  - MasterCard, IBM, Netscape
- STT (Secure Transaction Technology)
  - VISA, Microsoft

OBSOLETE

- SET (Secure Electronic Transactions)
  - MasterCard, VISA

VERY SLOW ACCEPTANCE

Secure Electronic Transaction (SET)

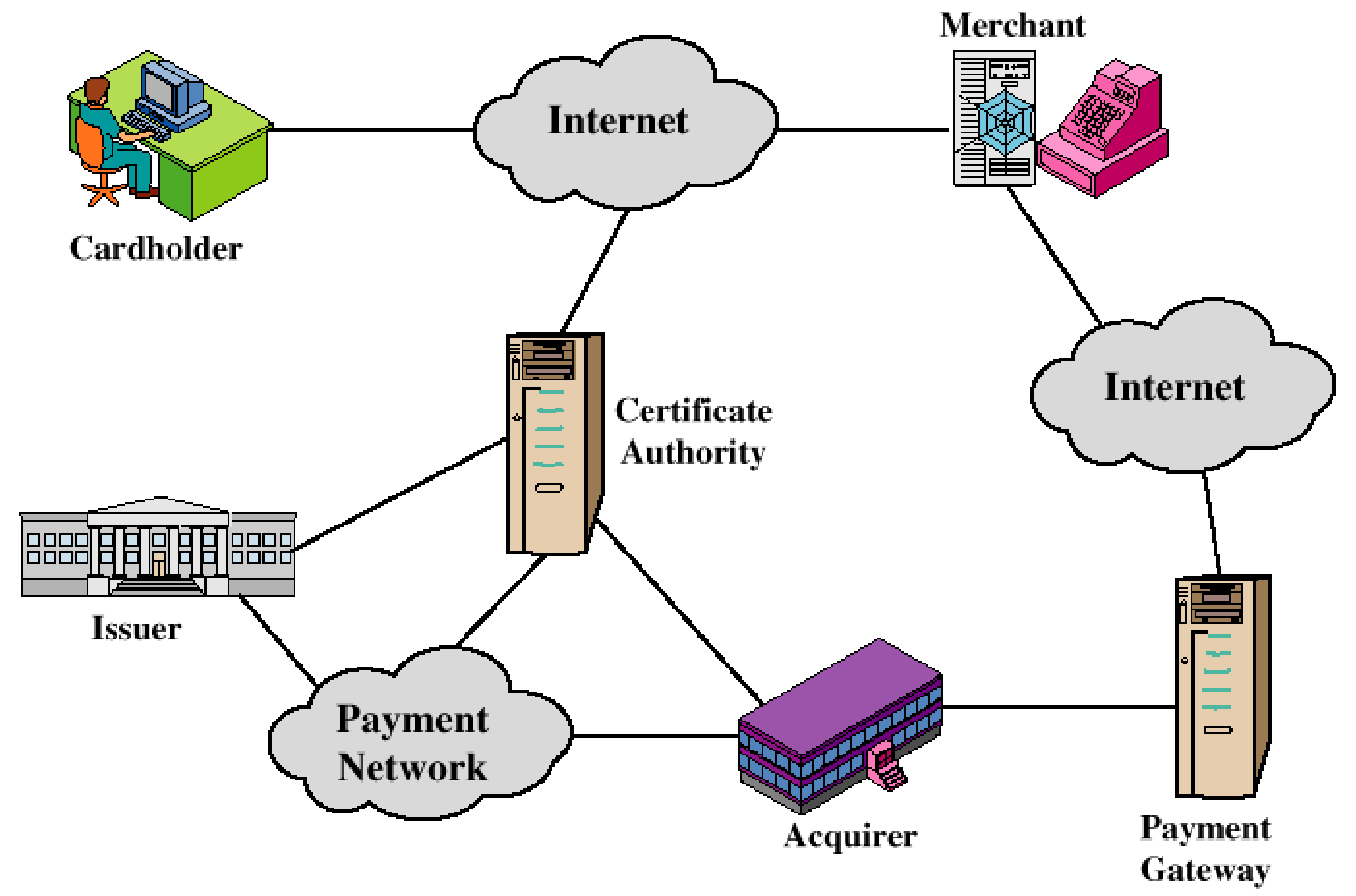
- **Developed by Visa and MasterCard**
- **Designed to protect credit card transactions**

- **Confidentiality: all messages encrypted**

- **Trust: all parties must have digital certificates**

- **Privacy: information made available only when and where necessary**

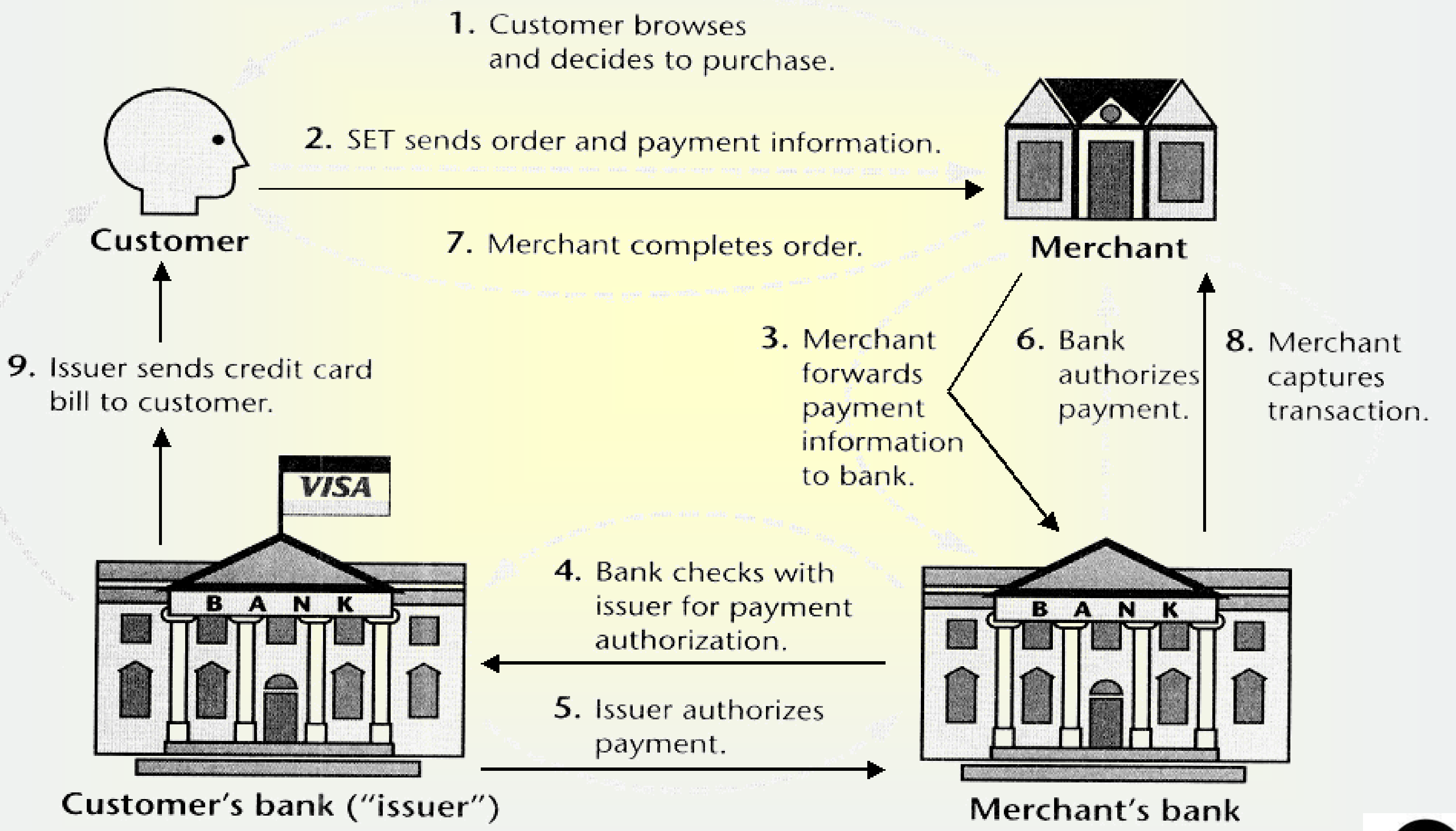
Participants in SET



SET Business Requirements

- Provide **confidentiality** of payment and ordering information
- Ensure the **integrity** of all transmitted data
- Provide **authentication** that a cardholder is a legitimate user of a credit card account
- Provide **authentication** that a merchant can accept credit card transactions through its relationship with a financial institution
- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction
- Create a protocol that neither depends on transport security mechanisms nor prevents their use
- Facilitate and encourage interoperability among software and network providers

SET Transactions


1. Customer browses and decides to purchase.
2. SET sends order and payment information.
7. Merchant completes order.
Customer
Merchant
9. Issuer sends credit card bill to customer.
3. Merchant forwards payment information to bank.
6. Bank authorizes payment.
8. Merchant captures transaction.
VISA
BANK
4. Bank checks with issuer for payment authorization.
5. Issuer authorizes payment.
BANK
Customer's bank ("issuer")
Merchant's bank

SET Transactions

- The following transaction protocols are defined in SET
  - card holder registration
  - merchant registration
  - purchase request
  - payment authorization
  - payment capture
  - certificate query
  - purchase inquiry
  - purchase notification
  - sale transaction
  - authorization reversal
  - capture reversal
  - credit reversal

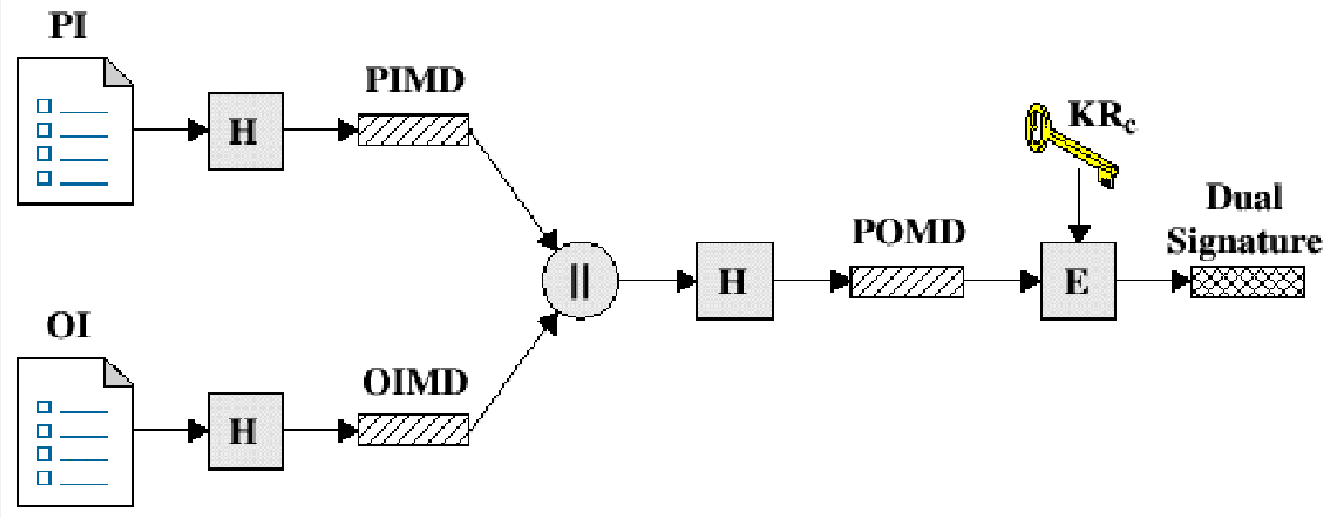
Key Technologies of SET

- Confidentiality of information: DES
- Integrity of data: RSA digital signatures with SHA-1 hash codes
- Cardholder account authentication: X.509v3 digital certificates with RSA signatures
- Merchant authentication: X.509v3 digital certificates with RSA signatures
- Privacy: separation of order and payment information using dual signatures

Dual Signatures

- Concept: Link Two Messages Intended for Two Different Receivers:
  - Order Information (OI): Customer to Merchant
  - Payment Information (PI): Customer to Bank
- Goal: Limit Information to A “Need-to-Know” Basis:
  - Merchant does not need credit card number.
  - Bank does not need details of customer order.
  - Afford the customer extra protection in terms of privacy by keeping these items separate.
- This **link** is needed to prove that payment is intended for this order and not some other one.
  - The merchant has received OI and verified the signature.
  - The bank has received PI and verified the signature.
  - The customer has linked the OI and PI and can prove the linkage.

Dual Signatures



- The operation for dual signature is as follows:
  - Take the hash (SHA-1) of the payment and order information.
  - These two hash values are concatenated [H(PI) || H(OI)] and then the result is hashed.
  - Customer encrypts the final hash with a private key creating the **dual signature**.

    $DS = E_{KRC} [H(H(PI) || H(OI))]$

4. Electronic Auctions

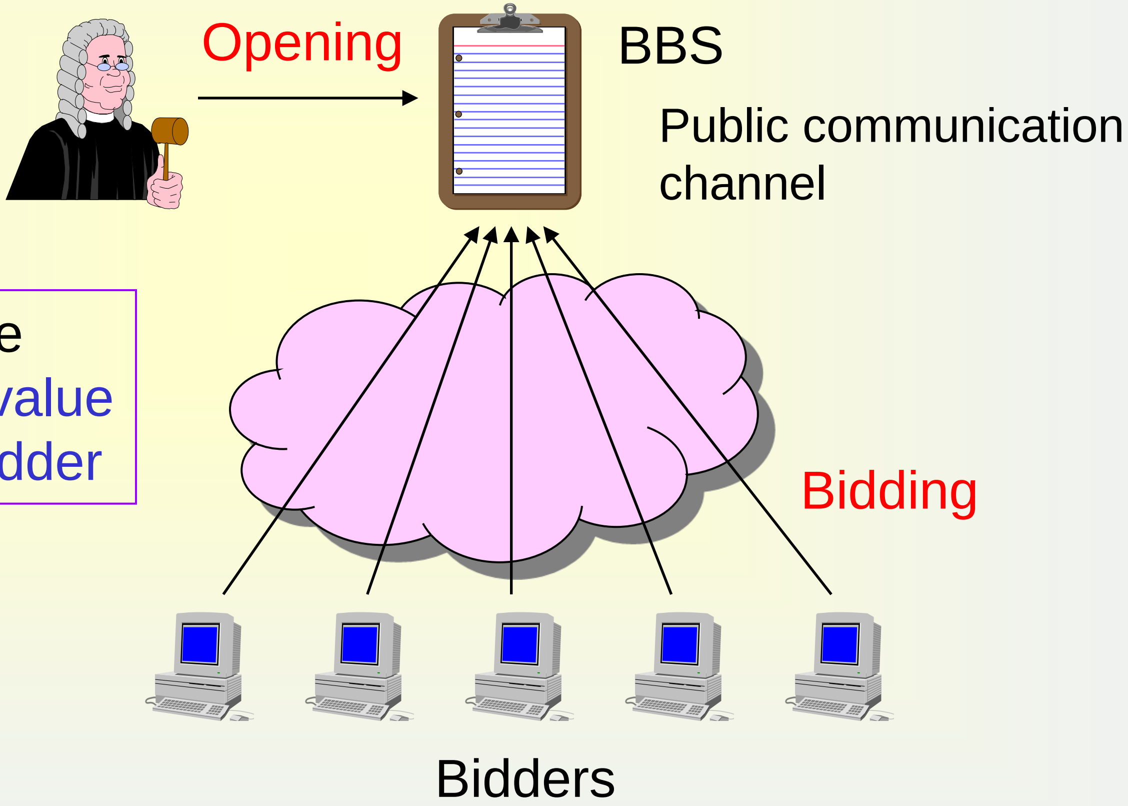
Auctions

- Auction is a competitive process in which either a seller solicits bids from buyers or a buyer solicits bids from sellers.
  - Negotiate price
  - Decide winner
  - Multi-party competition

- Auctions have a long history and is an effective method to distribute resources.

- Forward vs. reverse auction
  - Forward auctions are auctions that one seller uses as a channel to many potential buyers.
  - Reverse auctions are auctions that one buyer, usually an organization, wants to buy a product or service from many potential sellers.

Typical Model of Electronic Auction



Prime security issue

1. Secrecy of bid value
2. Anonymity of bidder

Real World Examples of Auction

- Sealed-bid auctions (비밀경매)
  - First priced sealed bid auction
  - Vickrey auction
  - Sealed double auction

- Public auctions (공개경매)
  - Dutch auction
  - English auction

Auction Types in the Real World

- **First priced sealed bid auction**
  - Rules (protocol): Bidders submit a single sealed bid before deadline
  - Outcome: Bidder with the highest bid price becomes the winner
- **Vickrey auction**
  - Rules (protocol): Bidders submit a single sealed bid before deadline
  - Outcome: Bidder with the highest bid price becomes the winner, but the second highest price becomes the price
- **Sealed double auction**
  - Rules (protocol): Bidders and sellers submit a single sealed bid before deadline
  - Outcome: Auctioneer determines a single market-clearing price and matches buyers and sellers

Auction Types in the Real World

- **Dutch auction**
  - Rules (protocol): Auctioneer calls out descending price. Bidder calls out a bid.
  - Outcome: Winner is the first bidder to call out at price bid

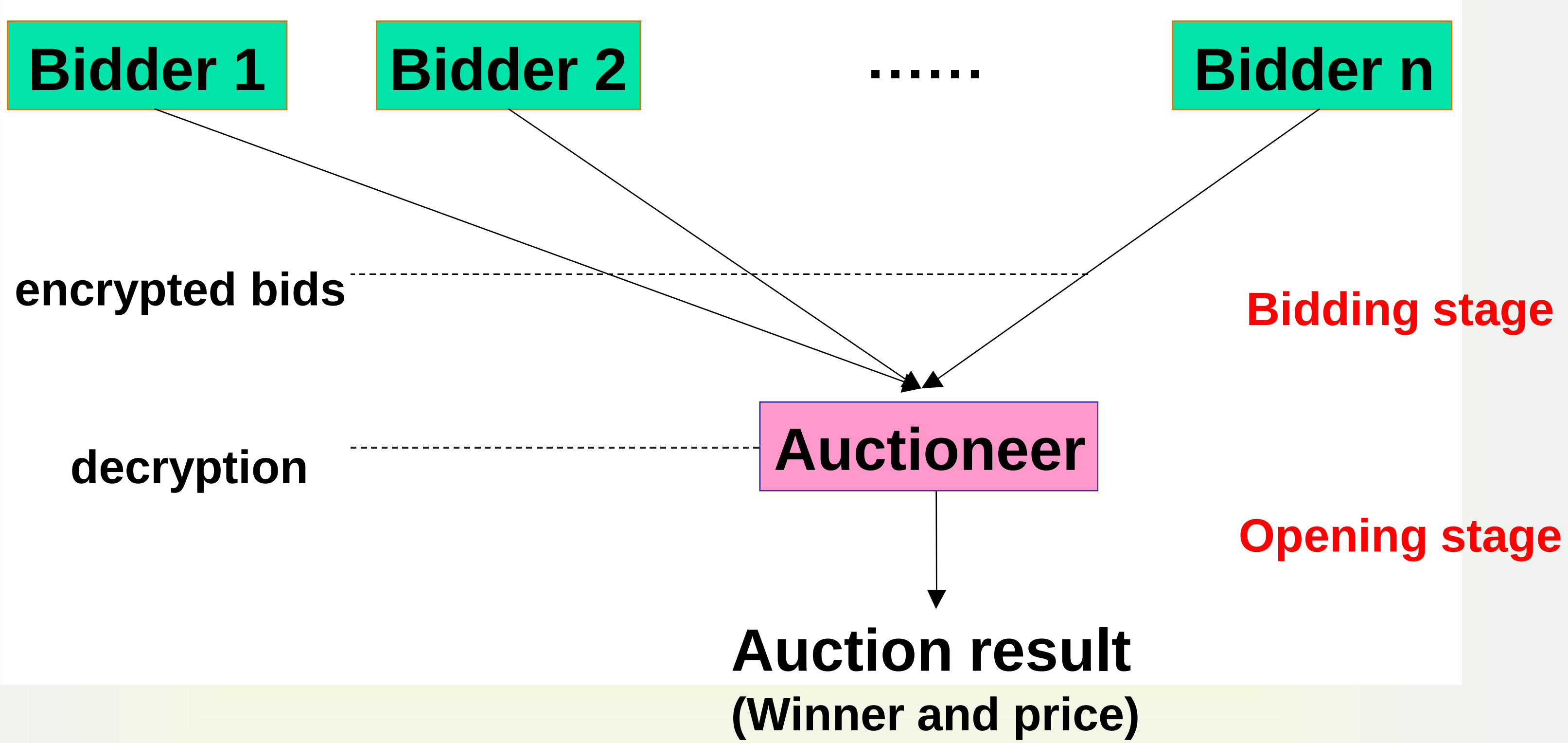
- **English auction**
  - Rules (protocol): Bidders successively raise bid for item until one bidder remains
  - Outcome: Winner is last bidder remaining at price of second-highest bidder

Cryptographic Implementation of Auctions

- Sealed-bid auction (비밀경매)
  - Provide Secrecy of bid value
  - Each bidder submits a bid only once secretly
  - Competition principle does not work well (A winning bid may be much higher than market price)

- Public auction (공개경매)
  - Provide Anonymity of bidder
  - Bidders participate in auction anonymously
  - Bidding values are published and multiple bidding is allowed
  - Familiar type of auction over the open network like the Internet
  - Many online auction services over the Internet

Sealed-bid Auctions



Bidder 1

Bidder 2

……

Bidder n

encrypted bids

Bidding stage

Auctioneer

decryption

Opening stage

Auction result

(Winner and price)

Requirements for Sealed-bid Auction

- Correctness: correct winning price and winners are determined according to the auction rule.
- Confidentiality: each bid remains confidential before the bid opening phase starts.
- Fairness: No bidder can choose his bid according to other bidders' bids.
- Robustness: Any malicious behaviour of any party cannot compromise the system or lead to an incorrect result.
- Public verifiability: correctness can be publicly verified.
- Non-repudiation: no bidder can deny his bid.
- Price Flexibility: the biddable prices are not limited to a small set. The bids can be as precise as the bidders like.
- Rule Flexibility: the auction protocol is independent of the auction rules.
- Privacy: confidentiality of the losing bids must be kept even after the bid opening phase.

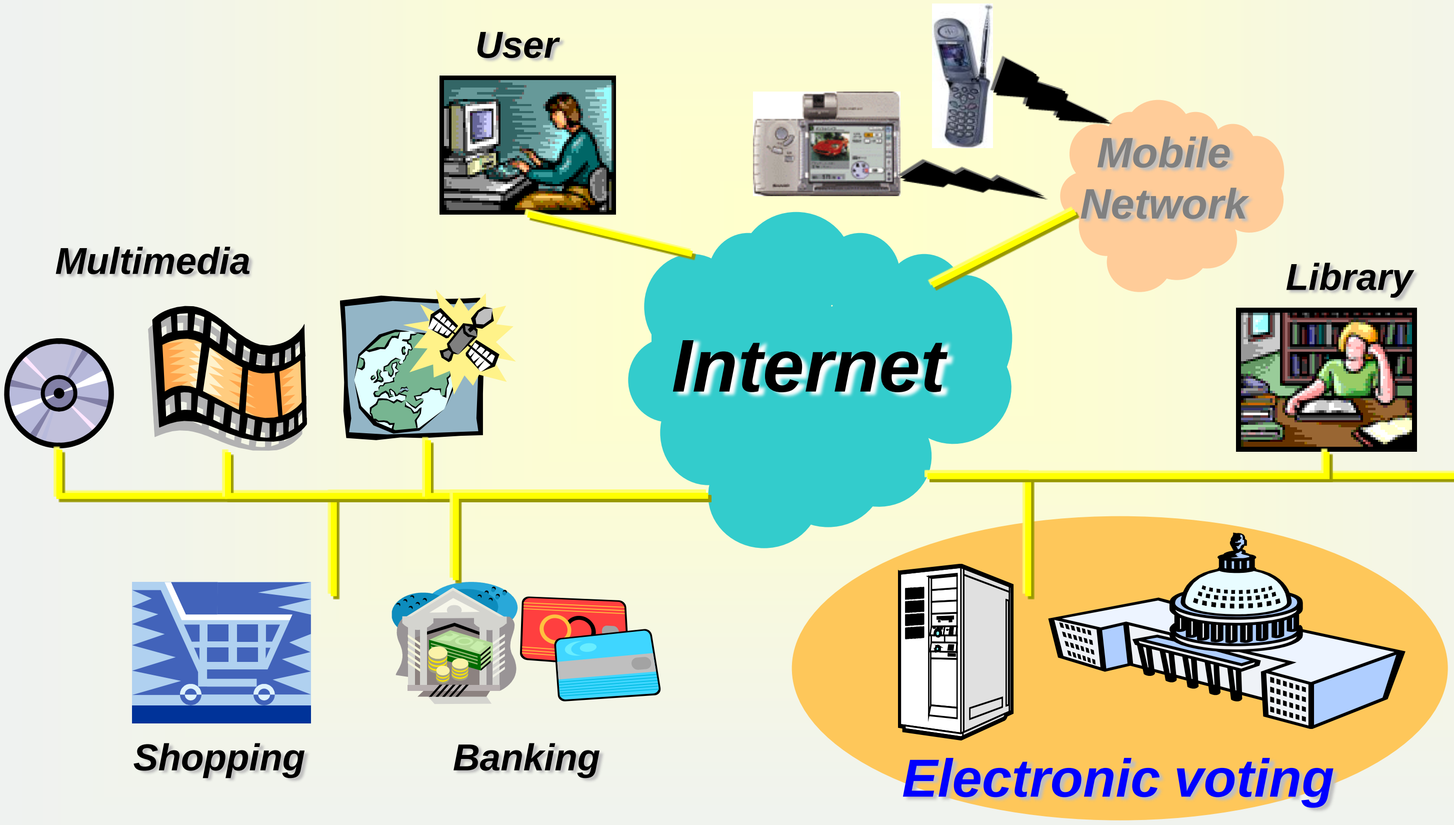
Requirements for Public Auction

- Anonymity
- Traceability (a winner is traceable after decision)
- No framing (nobody can impersonate a bidder)
- Unforgeability
- Non-repudiation
- Fairness (all bids should be fairly dealt with)
- Public verifiability
- Unlinkability among different auctions
- Linkability in an auction
- Efficiency of bidding
- One-time registration (can participate in multiple rounds)

5. Electronic Voting

Electronic Voting

- Implement real world voting (election) by electronic means (using computer and network)

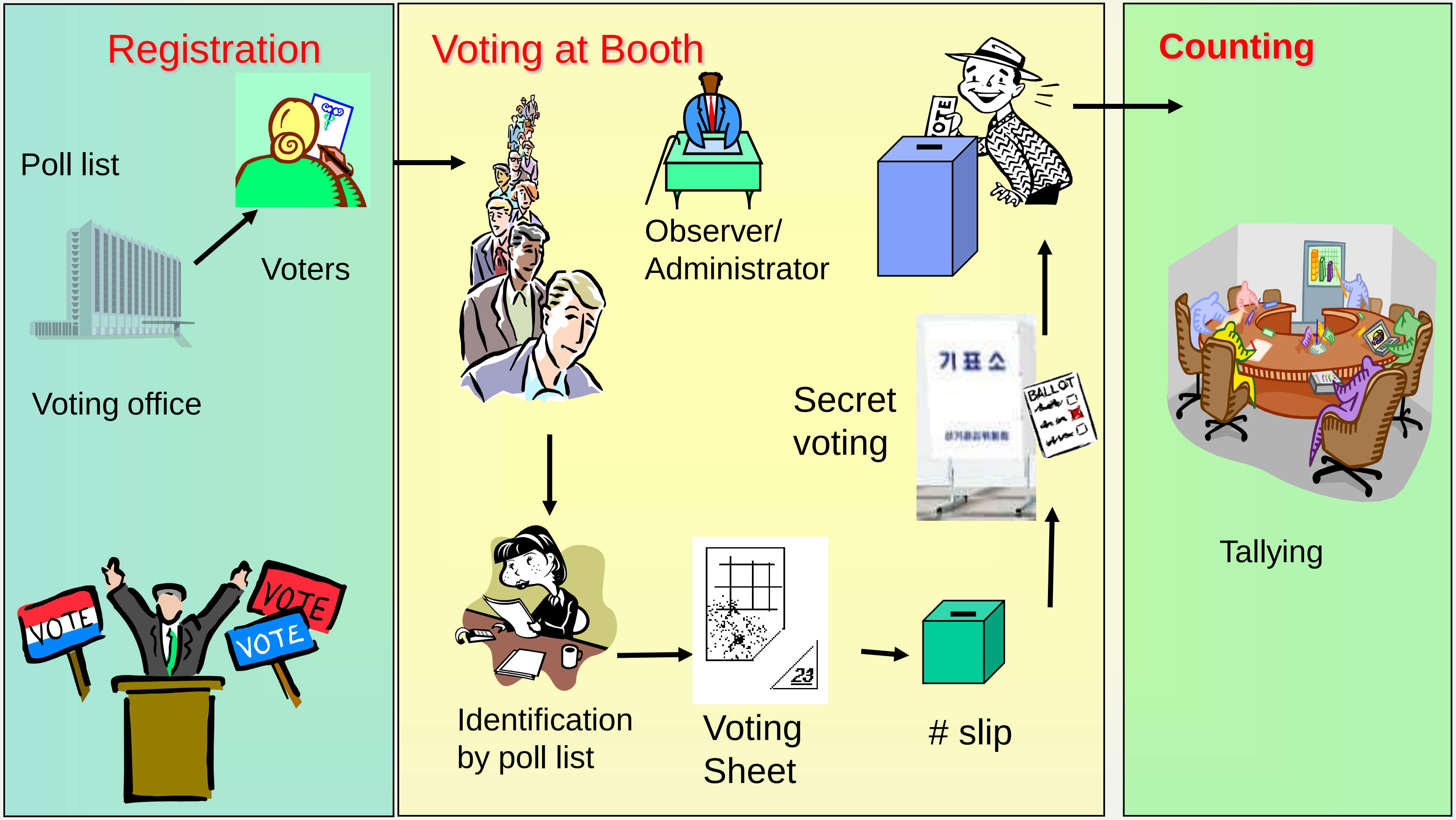


Why Electronic Voting?

- Advantages
  - Convenience for voters
  - Efficiency of management, counting
  - Provide alternative choice for voters rather than traditional paper-based voting

- Electronic voting can solve the problem of decreasing participation rate in voting. Younger generation prefers electronic means

Paper Voting Scenario



Registration

Poll list

Voters

Voting office

Voting at Booth

Observer/ Administrator

Secret voting

Identification by poll list

Voting Sheet

# slip

Counting

Tallying

Classification of Electronic Voting

- **Computer voting** (kiosk, electronic voting booth)
  - Electronic voting using computer in voting booth
  - Convenient user interface
  - Efficient management and tally
  - But, just half way to electronic voting

- **Internet voting**
  - Electronic voting using computers connected to the Internet
  - Can participate in voting in any place over the Internet
  - Proceeding to mobile voting

Electoral Systems

- **Plurality systems** (다수득표제)
  - Winner is who received the most votes regardless of majority requirement.
  - Winner takes all.
  - UK, Canada, USA
  - Single non-transferable vote : Japan
  - Block vote, Limited vote : Britain
  - Approval voting : USA

- **Majoritorian systems (결선투표제)**
  - Winner is required to receive more than half
  - Second ballot
  - Preferential voting (Alternative voting) in Australia

- **Many kinds of variants depending on cultural background**

Security Requirements of e-Voting

- Privacy (confidentiality)
- Prevention of double voting
- Universal verifiability (correctness)
- Fairness
- Robustness
- Receipt-freeness (prevent vote buying, coercion)

- Efficiency, Mobility, Convenience, Flexibility

Receipt-Freeness

- Receipt-freeness
  - A unique security requirement of electronic voting
  - Voter should not be able to construct a receipt
  - Voter must keep his vote private

- Why is it important?
  - Vote buying is a common experience in real political voting (threat, solicitation)

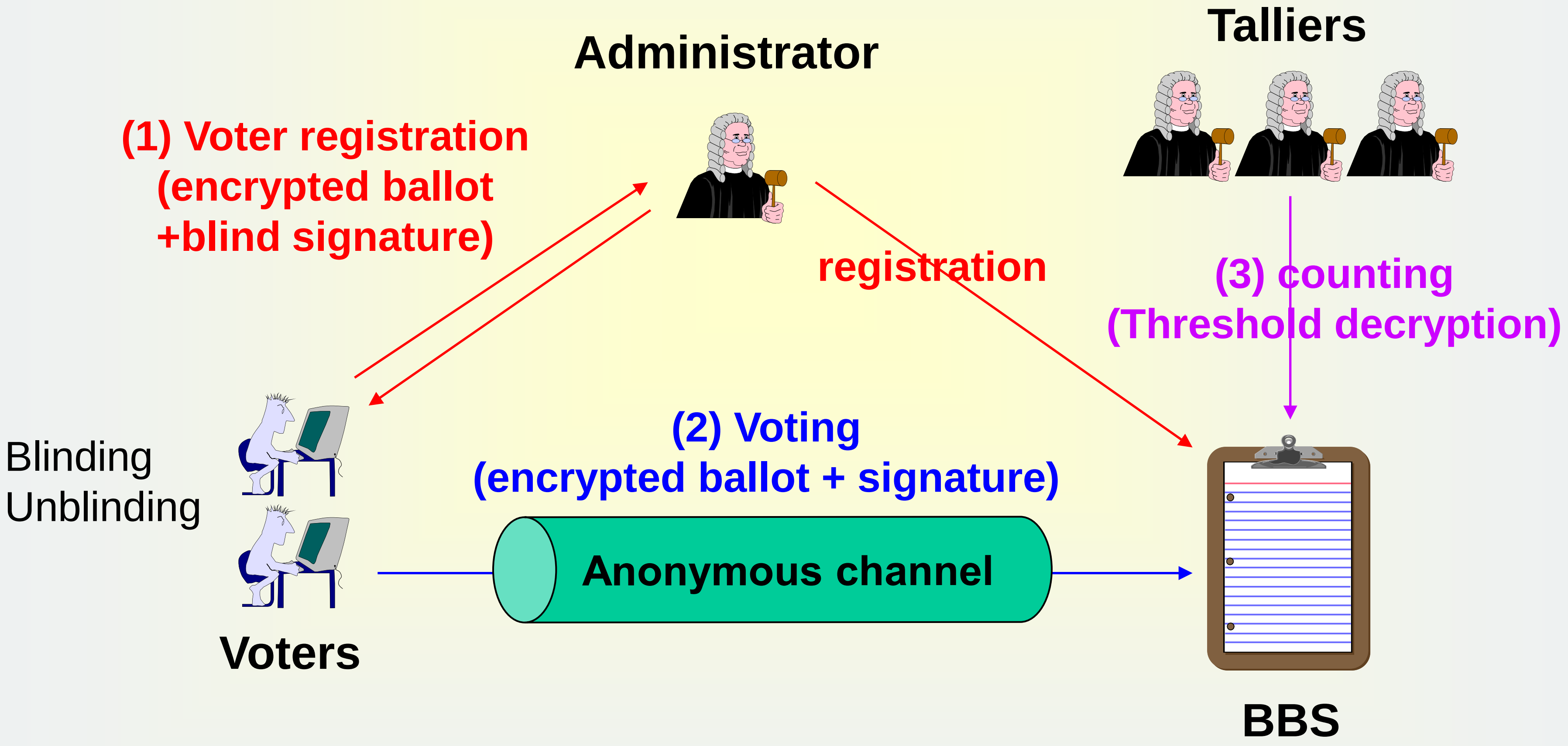
3 Approaches for Secure e-Voting

- Schemes using **blind signature**
  - Efficient, but requires anonymous channel (frequently implemented using mixnet)

- Schemes using **homomorphic encryption**
  - Huge proof size, restriction on message encoding
  - Many researches on receipt-freeness

- Schemes using **mixnet**
  - Require huge computation for mixing

e-Voting using Blind Signature



Administrator

Talliers

(1) Voter registration (encrypted ballot +blind signature)

registration

(3) counting (Threshold decryption)

Blinding
Unblinding

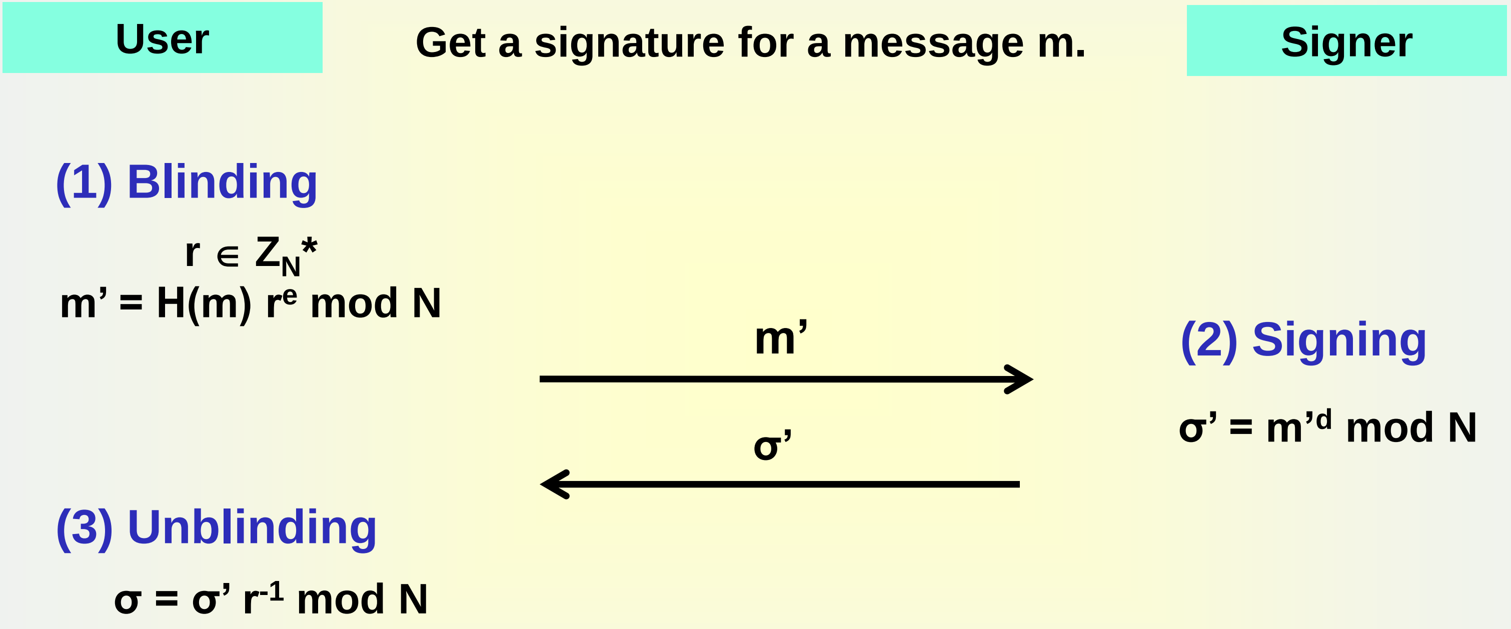
(2) Voting (encrypted ballot + signature)

Anonymous channel

Voters

BBS

RSA-based Blind Signature



User

Get a signature for a message m.

Signer

(1) Blinding

$r \in Z_N^*$

$m' = H(m)\, r^e \bmod N$

m'

(2) Signing

$\sigma' = m'^d \bmod N$

σ'

(3) Unblinding

$\sigma = \sigma'\, r^{-1} \bmod N$

$$\sigma = \sigma'\, r^{-1} \bmod N = (H(m)\, r^e)^d\, r^{-1} \bmod N = H(m)^d \bmod N$$

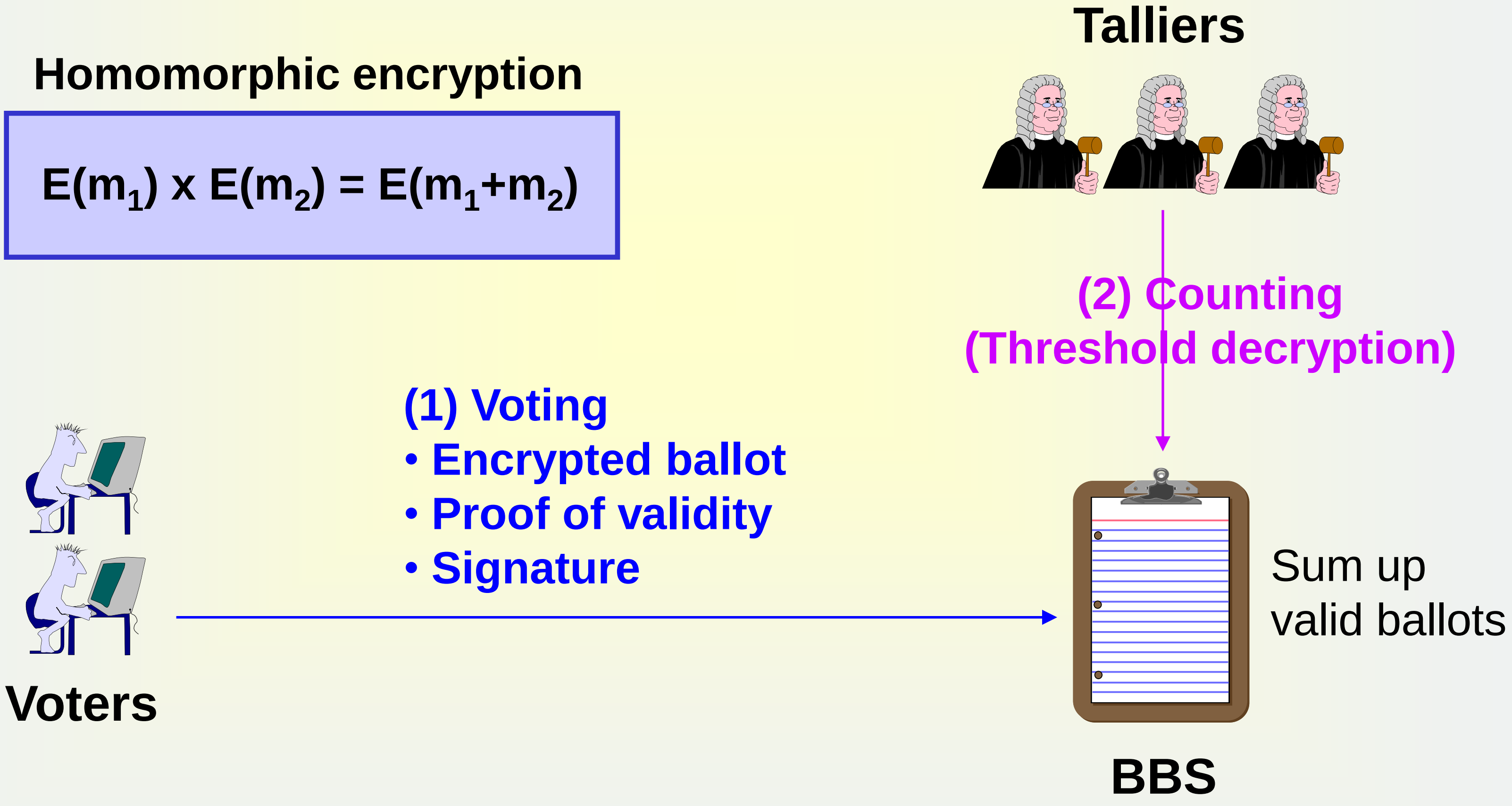
σ is a valid signature of the signer

The signer cannot have any information on m and σ.

e-Voting using Homomorphic Encryption

Homomorphic encryption

$$E(m_1) \times E(m_2) = E(m_1+m_2)$$



Talliers

(2) Counting
(Threshold decryption)

(1) Voting

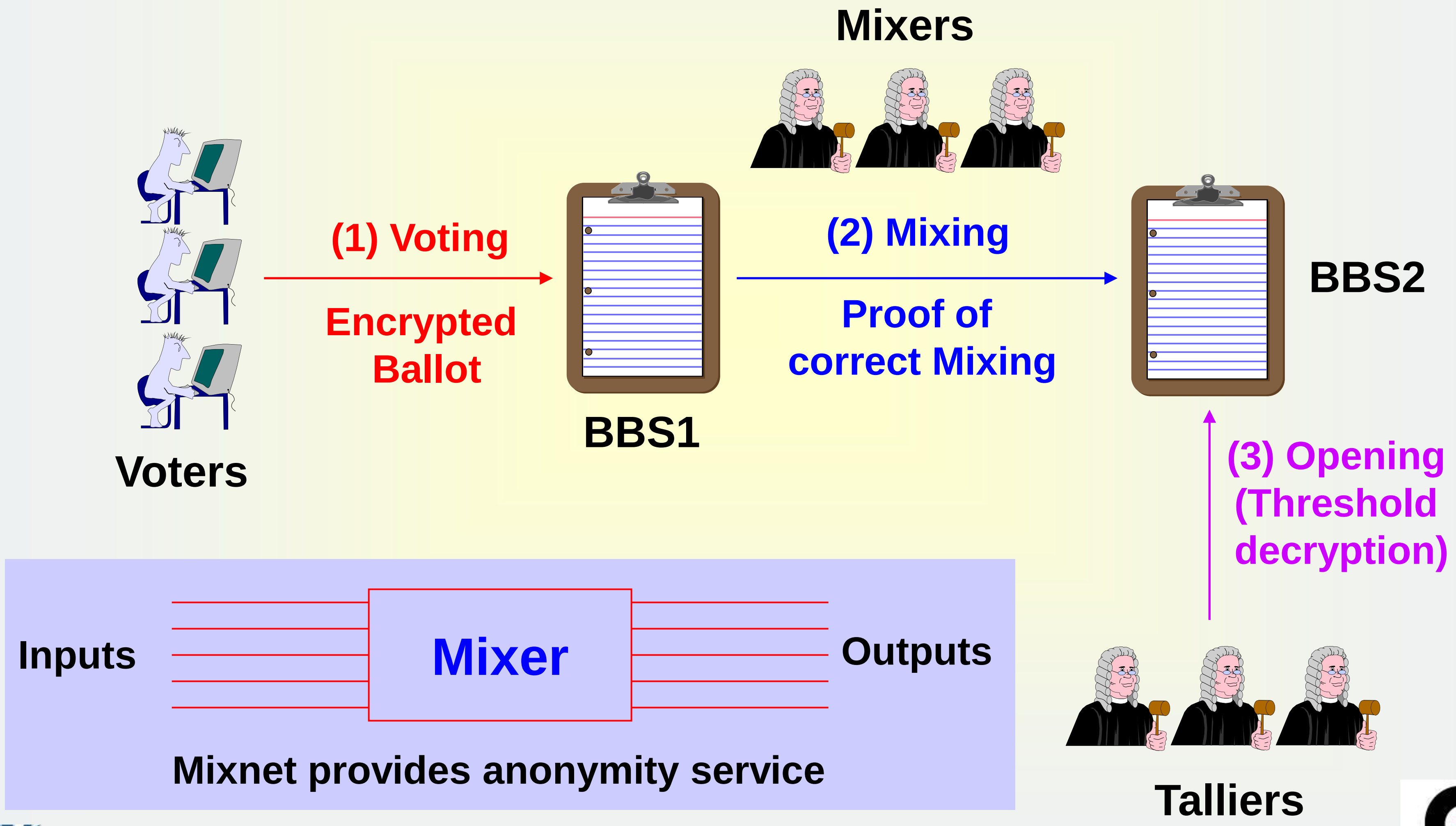
- **Encrypted ballot**
- **Proof of validity**
- **Signature**

Sum up
valid ballots

Voters

BBS

e-Voting using Mixnet



Voters

(1) Voting

Encrypted Ballot

BBS1

Mixers

(2) Mixing

Proof of correct Mixing

BBS2

(3) Opening (Threshold decryption)

Talliers

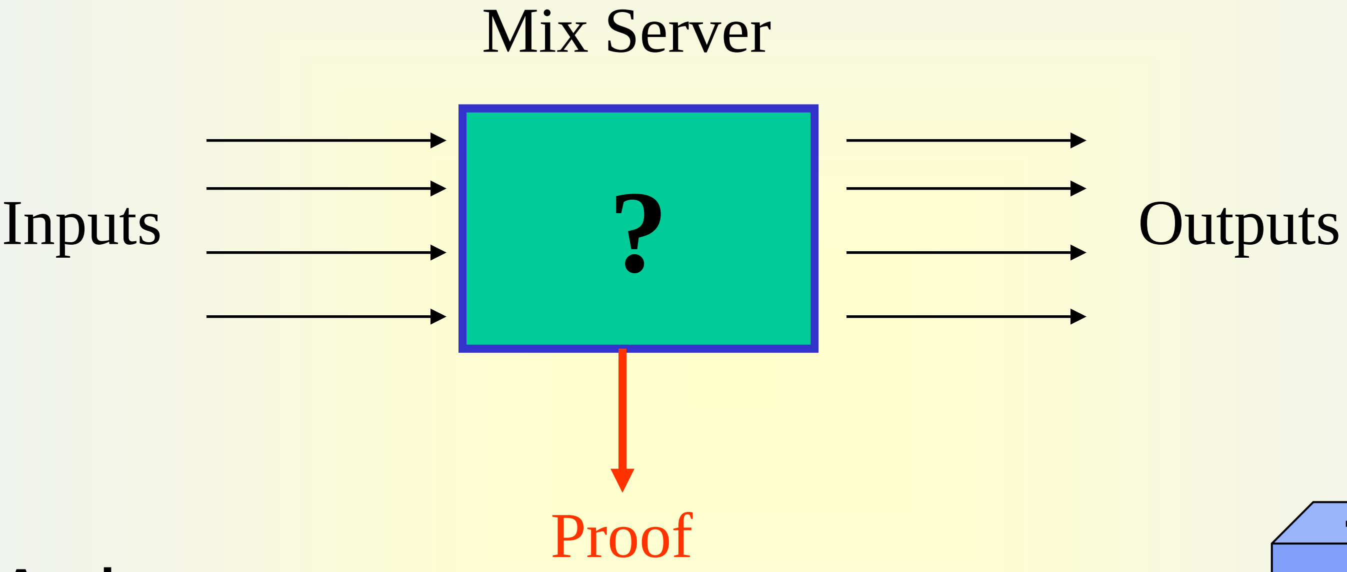
Inputs

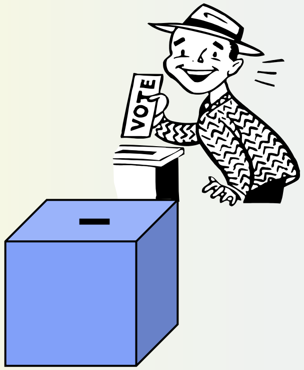
Mixer

Outputs

Mixnet provides anonymity service

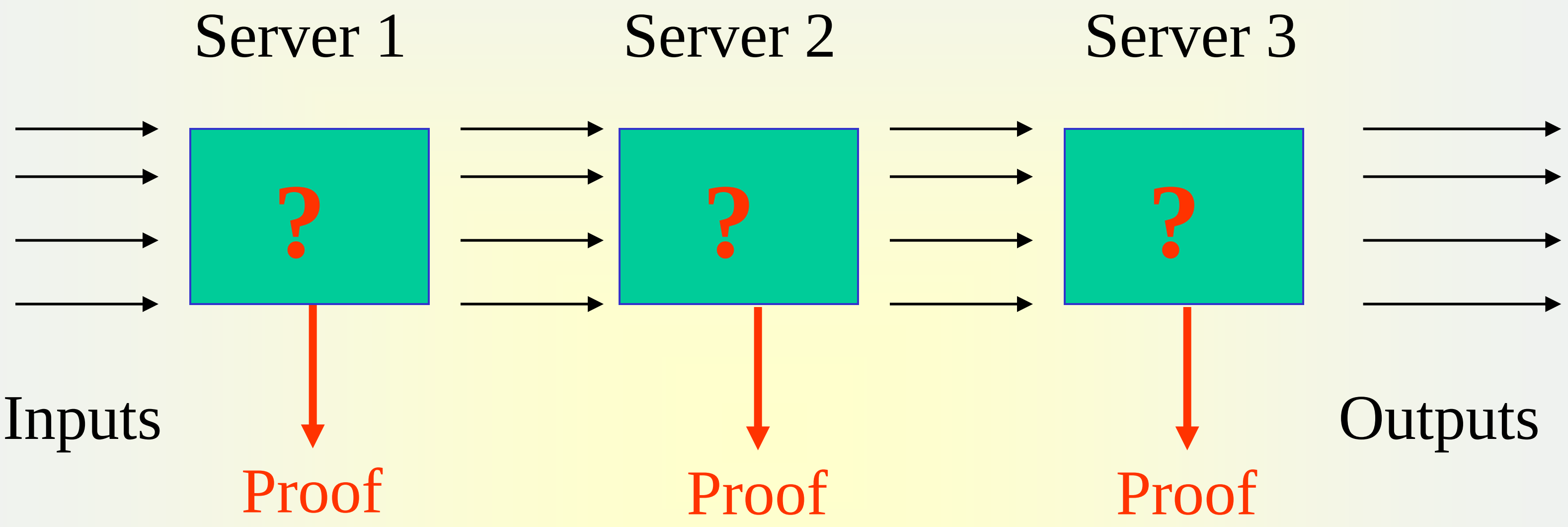
Mix Server





- A mix server:
  - Receives inputs
  - Produces “related” outputs
  - The relationship between inputs and outputs is secret
  - Cryptographic implementation of Ballot box

Mixnet



- **Mixnet (Mix network)**
  - **A group of mix servers that operate sequentially.**
  - **Provides anonymity service**

If a single mix server is honest, global permutation is secret.

Q & A

Thank you!