Public Key Infrastructure in India: Status and Issues

Palash Sarkar

Applied Statistics Unit
Indian Statistical Institute, Kolkata
India
palash@isical.ac.in

15th January, 2012



Structure of the Presentation

- A perspective.
- Digital signatures and digital certificates.
- IT Act and the enabling of PKI in India.
- Examples of e-protocols.
- Questions for information security researchers.



A Perspective



Digital World

A new way of interaction and communication.

- **e-commerce:** “consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks.” (Wikipedia)
- **e-government:** “the use of information and communication technology to provide and improve government services, transactions and interactions with citizens, businesses, and other arms of government.” (Wikipedia)

Counterpoint: agriculture will continue to be done in the fields.



Why E-Commerce?

There are lots of reasons. Primary among them would be the following.

- Convenience.
- Efficiency.
- A new medium opens up new possibilities.

Caveat: a new medium also opens up new pitfalls.



Paperless World

Assumption: whatever can be done using paper-based methods can be done digitally (in fact, much more can be done).

- As yet, we do not know whether this assumption is true.
- We are still at a fledgling stage.
- Efforts by governments and big businesses to reach the ideal.



Enabling E-Tasks

- Each e-task requires a protocol to achieve its goal.
- Different parties/players/users are involved.
- Each player has a pre-defined role.
- Need to ensure that a player sticks to the assigned role.
- This typically takes the form of a commitment by the player.
- Non-fulfillment of commitment brings upon legal punishment.



Commitment

- In the conventional world, a commitment is achieved by getting a player to sign a statement on a piece of paper.
- In the digital world, the same needs to be created (at least, to simulate the conventional world). This gives rise to **digital signatures**.
- This views the move from the conventional to the digital world as a bridging process.
- One may consider direct digitial methods; digital signatures would still remain relevant.



Digital Signatures and Digital Certificates



Cryptology: The Background Science

Two basic tasks.

- Encryption.
- Authentication.

Two basic notions.

- Conventional or classical notion: secret or symmetric key cryptosystems.
- Paradigm shift: asymmetric key cryptosystem (Diffie-Hellman, 1976).
  - Public key agreement.
  - Public key encryption.
  - Digital signature.
- In practice a combination is actually employed.



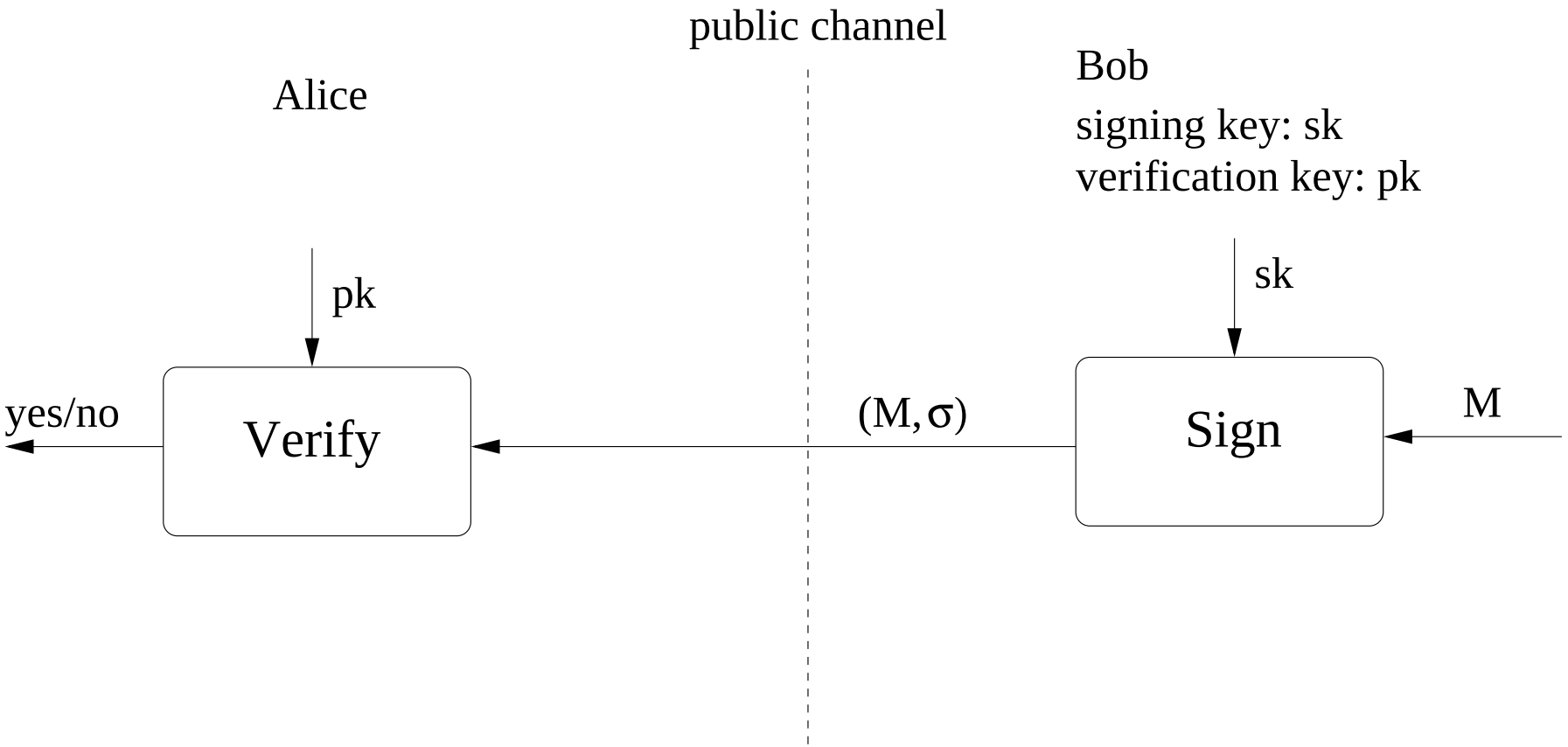
Digital Signature Schemes

Consists of three procedures: (Setup, Sign, Verify).

- **Setup:** generates (pk_B, sk_B) for Bob;
  pk_B is made public (placed in a public directory).
- **Sign:** Bob signs message M using sk_B to obtain signature σ.
- **Verify:** Alice can verify the validity of (M, σ) using pk_B;
  Alice does not need any secret information to verify a signature.



Overview of Signature Scheme



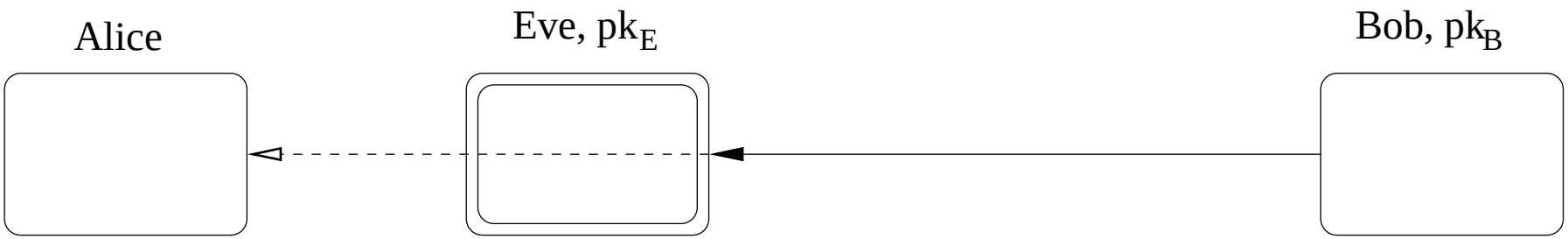
(Wo)man in the Middle

- Eve impersonates Bob.
- Puts a public key pk_E in the name of Bob.
- Eve signs a message M using sk_E.
- Alice verifies the signature using pk_E that she thinks is Bob's public key.

Question: when can Bob *trust* that the public key is indeed that of Alice?



How to Trust a Public Key?



Certifying Authority

- A CA has a key pair (pk_C, sk_C).
- Bob obtains certificate.
  - Bob generates (pk_B, sk_B); sends pk_B to CA.
  - CA signs (Bob, pk_B) using sk_C to obtain σ_B; Bob's certificate: (Bob, pk_B, σ_B).
- Alice verifies (M, σ) signed by Bob.
  - Verifies (Bob, pk_B, σ_B) using pk_C.
  - Verifies (M, σ) using pk_B.
- **Trust:**
  - Alice trusts pk_C;
  - hence, Alice trusts pk_B.



Management of Certificates

- A CA may revoke Bob's certificate.
  - Bob has lost her private key.
  - The validity of the certificate has expired.
  - Other reasons?
- Alice needs to know whether Bob's certificate is "fresh".
  - Certificate revocation list (CRL).
  - Online certificate status protocol (OCSP).
  - One-way hash chains.

Public Key Infrastructure (PKI) covers all of the above.



X.509 Certificate Format

- version number
- serial number
- signature algorithm ID
- issuer name
- validity period
- subject name (i.e., certificate owner)
- certificate owner's public key
- optional fields
- the CA's signature on all previous fields



The Legal Angle

- For digital signatures to be accepted, the law has to recognise these as legal.
- United Nations Commission on International Trade Law (UNCITRAL).
  - Formulated a model law on e-commerce in 1996.
  - Adopted by the General Assembly resolution 51/162 of 16 December 1996.

"Recommends that all States give favourable consideration to the Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;"



IT Act and the Enabling of PKI in India

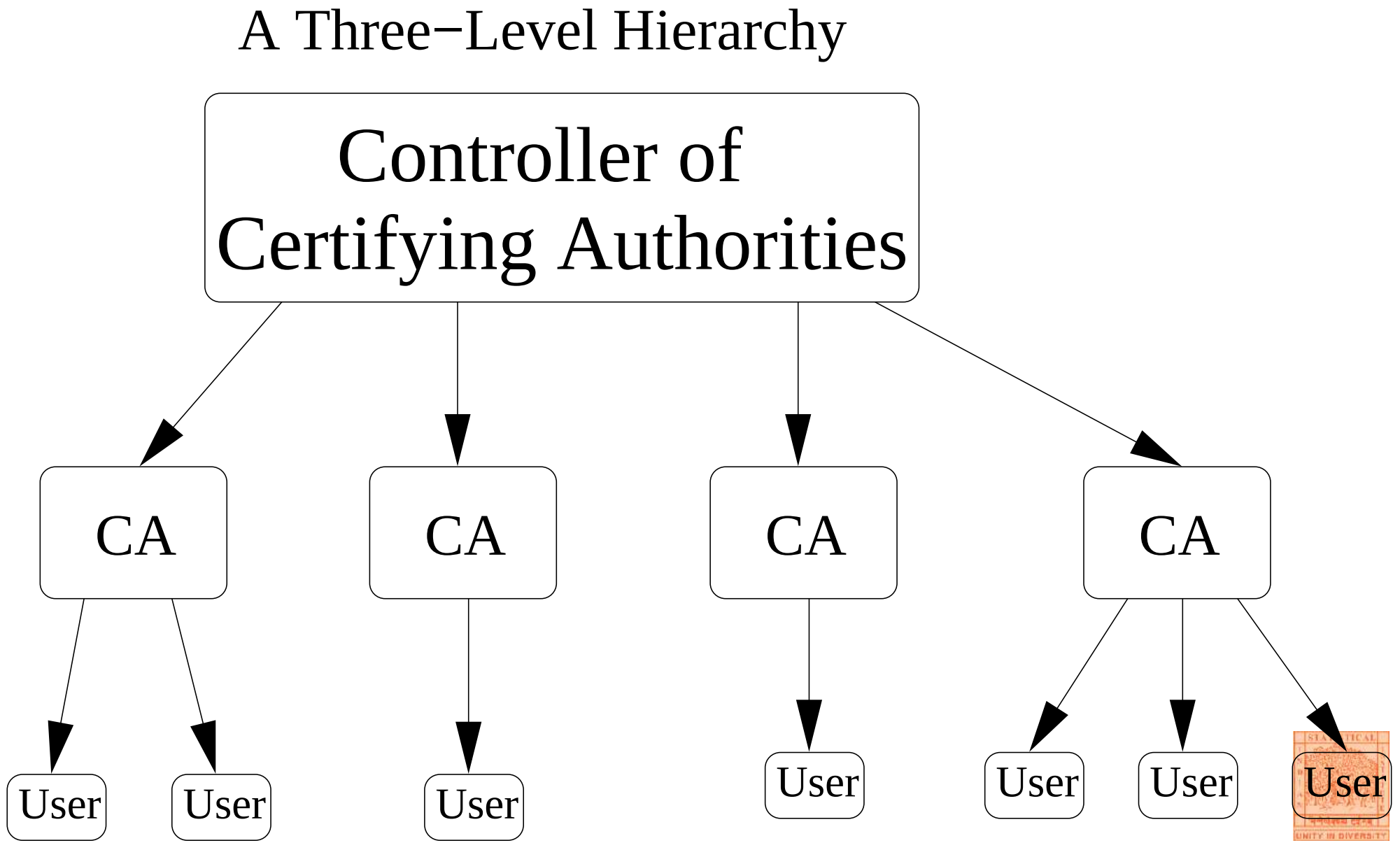


Indian IT Act, 2000, 2006

- Provides legal sanctity to digital signatures based upon the principle of equivalence to handwritten signatures.
- Provides for the creation and management of PKI in India.
- Cascaded amendments to several other acts.
  - Indian Evidence Act, 1872.
  - Banker's Book Evidence Act, 1891.
  - Reserve Bank of India Act, 1934.
  - Indian Penal Code.
- Covers aspects other than digital signatures.
  - Issues related to digital distribution of obscenity.
  - Issues related to wire-tapping by governmental agencies.



PKI-India Framework



Three-Level Hierarchy

- The CCA (or root CA) only issues certificates to CAs.
- The CAs issue certificates to individual users.
  - Certain CAs issue certificates to certain category of users.
- There are no lower level CAs, i.e., a CA cannot issue a certificate to another CA.
- Trust in a certificate is ultimately derived from the root CA.
- Cross-certification with a foreign CA.
  - An individual CA can arrange for cross-certification after due approval by the CCA, India.



Functions of the CCA

- Creation and maintenance of the Root CA of India (RCAI).
  - Root CA certificate is a self-signed certificate. It is based on the ITU-T X.509 standard.
  - Protection of private key of CCA (using tamper proof hardware and 3-out-of-3 access control).
- Issue certificates to individual CAs.
- Maintain the national repository of digital certificates (NRDC) (mandated under Section 20 of the IT Act): copies of all certificates and certificate revocation lists.
- Empanel auditors for auditing infrastructure of CAs.
- Generally act as the controlling authority of all PKI-related issues in India.



Standards Notified in India

- **Internet Engineering Task Force (IETF):** Internet X.509 Public Key Infrastructure.
- **IEEE standard P1363 for three families:** Discrete Logarithm (DL) systems; Elliptic Curve Discrete Logarithm (EC) systems; Integer Factorization (IF) systems.
- **Public-key Cryptography Standards (PKCS):** numbers 1,3,5,6,7,8,9,10,11,12,13 and 15.
- **Federal Information Processing Standards (FIPS):** FIPS 180-1, Secure Hash Standard; FIPS 186-1, Digital Signature Standard (DSS). FIPS 140-1 level 3, Security Requirement for Cryptographic Modules.
- **Discrete Logarithm (DL) systems:** Diffie-Hellman, MQV key agreement; DSA, Nyberg-Rueppel signatures.



Standards Notified in India (contd.)

- **Elliptic Curve (EC) systems:** elliptic curve analogs of DL systems.
- **Integer Factorization (IF) systems:** RSA encryption; RSA, Rabin-Williams signatures.
- **Key agreement schemes.**
- **Signature schemes:** DL/EC scheme with message recovery; PSS, FDH, PKCS #1 encoding methods for IF family; PSS-R for message recovery in IF family.
- **Encryption schemes:** Abdalla-Bellare-Rogaway DHAES for DL/EC family.



Rules Governing Key Pairs

- **CA:** at least 2048-bit RSA keys;
  users: at least 1024-bit RSA keys.
- CA has to change key pair every 3 to 5 years as per certificate practice statement (CPS) guidelines.
- Subscriber's key pair should be changed every 1 to 2 years.



CAs in India

Information as of 2009.



CAs in India

Information as of 2009.

- **Safescrypt:** private sector.
- **IDRBT:** issues certificates to the banking sector.
- **National Informatics Centre:** issues certificates to the government sector.
- **TCS:** private sector.
- **Customs and Central Excise:** government department.
- **MTNL:** telecom sector.
- **GNFC, (n)Code:** private sector.
- **e-Mudhra:** private sector.

More than 50,000 certificates have issued (as of 2009).



Classes of Certificates

- **Class 0:** issued only for demonstration/test purposes.
- **Class 1:** issued to individuals/private subscribers; confirms that user's name (or alias) and e-mail address form an unambiguous subject within the CA's database.
- **Class 2:** issued for both business personnel and private individuals use; confirms that the information in the application provided by the user does not conflict with the information in well-recognized consumer databases.
- **Class 3:** issued to individuals as well as organizations; high assurance certificates, intended for e-commerce applications; issued to individuals only on their personal (physical) appearance before the CA.
- A CA may issue other classes of certificates, provided purpose and verification method is explicitly outlined.



Examples of E-Protocols



Examples of E-Protocols

- **E-Procurement.**
  - **Air India:** online bidding for all purchase categories (1st April, 2009); no paper bids accepted for tenders against whom online bids have been invited.
  - **Northern Railways:** started from May, 2005;
    - covers all types of tenders issued by engineering (works) and stores department of NR;
    - tender notices are published on NR's website;
    - offers are submitted electronically with digital signatures;
    - tenderers can see the tabulation statement of all offers after opening of advertised tenders and also the status of their tenders;
    - security money is deposited electronically through a payment gateway;
    - information regarding purchase order is conveyed to the concerned vendors through e-mail.

  Source: A. K. Jain, S. Jain, e-Procurement in Indian Railways.



Examples of E-Protocols

- **Financial Services.**
  - National Securities Depository Limited (NSDL): **speed-e** service;
    - A demat account holder can access NSDL through speed-e;
    - access for clearing members only through smart cards;
    - authentication by digital signatures which are embedded in the smart card;
    - after authorization, a demat account holder can issue clearing instructions.
  - Central Depository Services (India) Limited (CDSL).
- **Stock exchanges.**
  - National Stock Exchange: apparently works as sub-CA for Safescrypt-CA.
  - Bombay Stock Exchange: works as sub-CA for TCS-CA, issuing certificates to its members.
- E-Contract notes as per SEBI guidelines.



Examples of E-Protocols

- **Banking Services.**
  - **Indian Financial Network (INFINET)** by IDRBT: countrywide communication backbone for the banks and financial institutions for payment system;
    - INFINET established by IDRBT;
    - membership open to the Reserve Bank of India, public sector banks, private banks, foreign banks, cooperative banks and financial institutions in India;
    - IDRBT-CA is licensed to issue certificates to members of INFINET.
  - **Structured financial messaging systems (SFMS):** securing inter/intra bank messaging systems for applications such as money transfer.
  - **Corporate internet banking:** by banks like ICICI, Punjab National Bank.



Examples of E-Protocols

- **Government.**
  - **Ministry of Commerce and Industries:** e-Application and approvals for special economic zones (SEZ) and export oriented units;
  - **Income Tax department:** online tax returns through e-intermediaries.
  - **Railway ticketing agent:** authentication via user-id/password and digital certificates to access the railway reservation network.



e-Payment System: Government of India

According to a PIB release on 28th October, 2011, the GOI has launched an e-Payment System (`http://pib.nic.in/newsite/erelease.aspx?relid=76885`).

- Developed by Controller General of Accounts (CGA), Department of Expenditure, Ministry of Finance.
- For payment of direct credit of dues from the Government of India into the account of beneficiaries.
- Uses digitally signed electronic advice (e-advice) through the 'Government e-Payment Gateway' (GePG).
- Goals:
  - Will bring transparency and expedite direct payments.
  - Direct payment of subsidies to the users and consumers of fertilizer, kerosene and cooking gas.
  - Increase the adoption of other e-services.



e-Governance in India: Some Links

MIT-CCA: `http://www.mit.gov.in/content/cca`

- e-Governance:
  `http://www.mit.gov.in/content/e-governance.`
- Projects and Initiatives
  `http://www.mit.gov.in/content/projects-and-initiatives.`
- Acts and Policies:
  `http://www.mit.gov.in/content/acts-policies.`



Questions for Information Security Researchers



From the IT Act

"If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was –

(a) unique to the subscriber affixing it;

(b) capable of identifying such subscriber;

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered then digital signature would be invalidated,

then such digital signature shall be deemed to be a secure digital signature."



From the IT Act

"If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was –

(a) unique to the subscriber affixing it;

(b) capable of identifying such subscriber;

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered then digital signature would be invalidated,

then such digital signature shall be deemed to be a secure digital signature."

Question. What is the relationship of the above to the scientific definition of secure digital signature?



From the IT Act

"A has a letter of credit upon B for Rupees 10,000, written by Z. A, in order to defraud B, adds a cipher to the 10,000, and makes the sum 1,00,000 intending that it may be believed by B that Z so wrote the letter. A has committed forgery."

"A signs his own name to a bill of exchange, intending that it may be believed that the bill was drawn by another person of the same name. A has committed forgery."

There are 16 such illustrations.



From the IT Act

"A has a letter of credit upon B for Rupees 10,000, written by Z. A, in order to defraud B, adds a cipher to the 10,000, and makes the sum 1,00,000 intending that it may be believed by B that Z so wrote the letter. A has committed forgery."

"A signs his own name to a bill of exchange, intending that it may be believed that the bill was drawn by another person of the same name. A has committed forgery."

There are 16 such illustrations.

Question: Can one come up with a good explanation of how and why the scientific definition of secure digital signature rules out these and similar cases?



Digital Signatures Galore

There are many variants of digital signatures.

- Blind, unique, ring, aggregate, multi-signature, proxy, deniable, ...
- Identity-based versions.



Digital Signatures Galore

There are many variants of digital signatures.

- Blind, unique, ring, aggregate, multi-signature, proxy, deniable, ...
- Identity-based versions.

Papers introducing variants provide some motivation.



Digital Signatures Galore

There are many variants of digital signatures.

- Blind, unique, ring, aggregate, multi-signature, proxy, deniable, ...
- Identity-based versions.

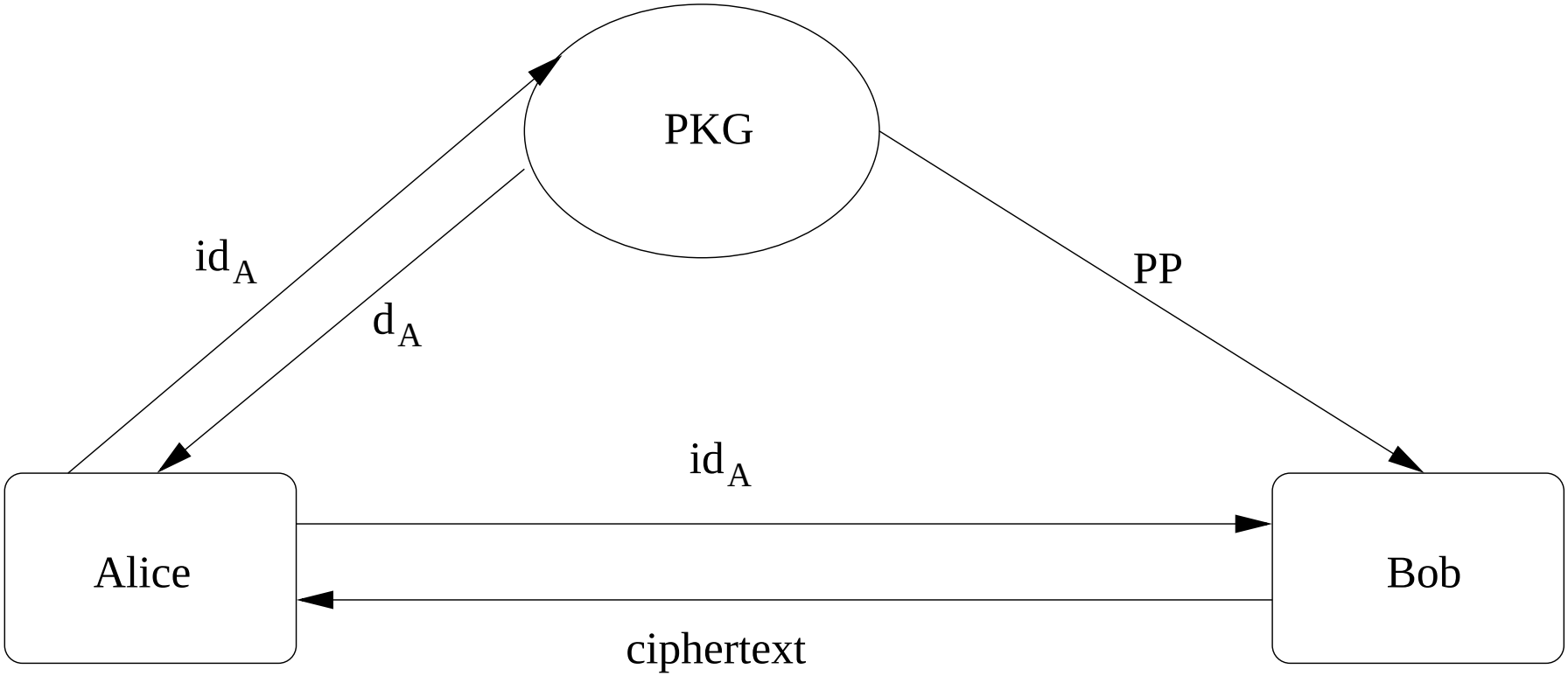
Papers introducing variants provide some motivation.

Problems:

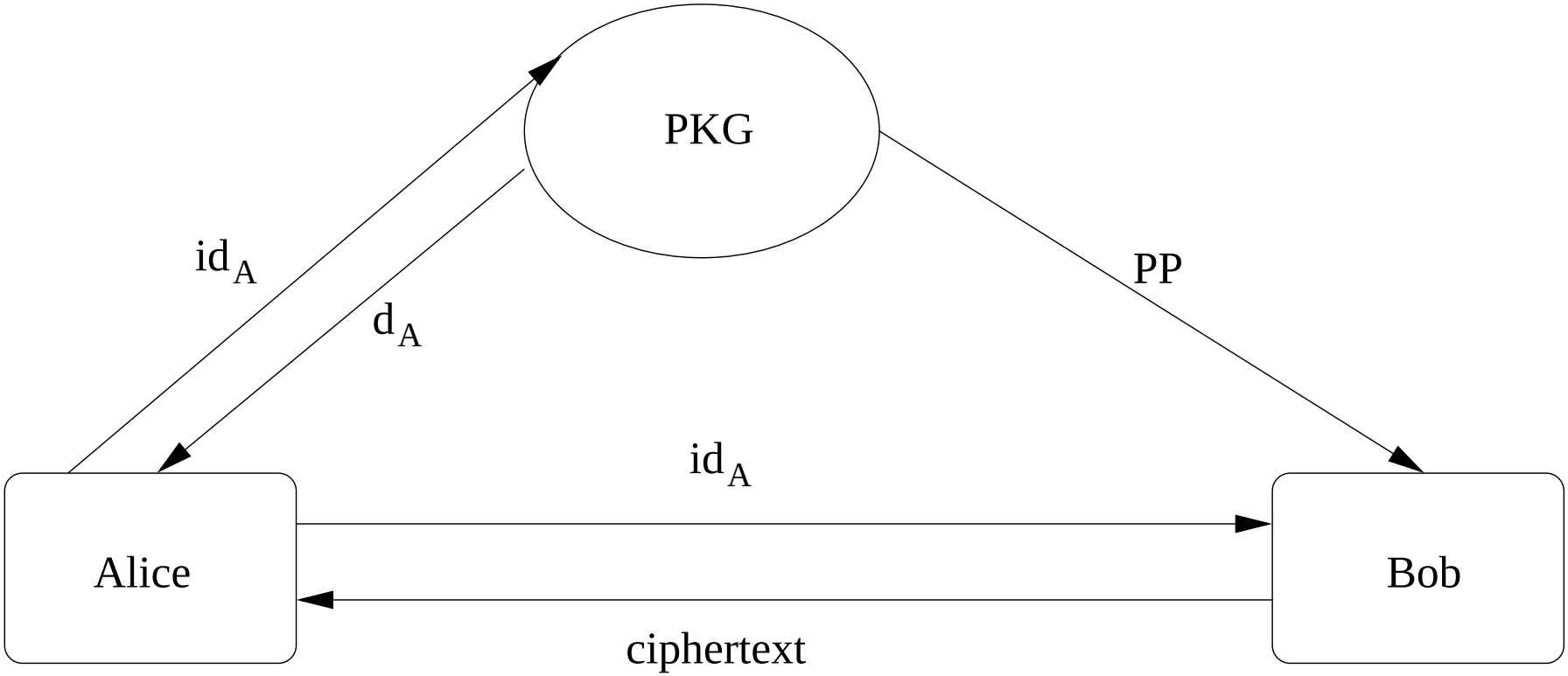
- For complex real-life examples identify appropriate portions where suitable variants can be fitted.
- Come up with general principles of mapping signature variants to applications.



Identity-Based Encryption



Hierarchical Identity-Based Encryption



Should HIBE be Deployed in India?

- HIBE has the potential to reduce/simplify issues of certificate management.
  - If not replace, HIBE may mitigate PKI-related problems.
  - May be ideal for small ‘niche’ applications.



Should HIBE be Deployed in India?

- HIBE has the potential to reduce/simplify issues of certificate management.
  - If not replace, HIBE may mitigate PKI-related problems.
  - May be ideal for small ‘niche’ applications.
- The 3-level PKI framework can very easily double as a 3-level HIBE:
  - the CCA works as the root private key generator (PKG);
  - the second level CAs issues private keys corresponding to identities;
  - the third level are the actual users.



Should HIBE be Deployed in India?

- HIBE has the potential to reduce/simplify issues of certificate management.
  - If not replace, HIBE may mitigate PKI-related problems.
  - May be ideal for small ‘niche’ applications.
- The 3-level PKI framework can very easily double as a 3-level HIBE:
  - the CCA works as the root private key generator (PKG);
  - the second level CAs issues private keys corresponding to identities;
  - the third level are the actual users.
- Key escrow:
  - inherent in (H)IBE framework;
  - can be overcome using different approaches:
    - sharing of master secret key of the PKG;
    - certificate-less encryption/certificate-based encryption;
    - other methods ...



Protocol Analysis

- Usual approach: protocols and security definitions, protocol specifications, detailed proofs of security reductions.
- Appearance of new protocols will raise new challenges for this approach.
- Alternative approach:
  - logic based specification and automated tools for analysis;
  - challenge: may require new logic modalities;
  - how far can this approach be relied upon?
- Both approaches are at certain levels of abstractions.
- How to verify actual implementations?



Analysis of Deployed Systems

Several large projects have already been deployed.

- Example: Government e-Payment Gateway.

A detailed and threadbare analysis of these systems is the call of the day for information security researchers.

- Even a small (and subtle) security flaw can lead to catastrophic consequences.
- Study of large complex security systems is really an ongoing process.
  - Especially since one can hardly *prove* such systems to be secure.
- Academicians have a role to play.
  - Potentially a huge area of research.



Opportunities for Innovative Applications

Rapid development of mobile communication technology and the fast disappearing digital divide.



Opportunities for Innovative Applications

Rapid development of mobile communication technology and the fast disappearing digital divide.

Online services over mobile phones can now be leveraged in the villages.



Opportunities for Innovative Applications

Rapid development of mobile communication technology and the fast disappearing digital divide.

Online services over mobile phones can now be leveraged in the villages.
Opens up possibilities for new business applications geared towards rural India.

- **Rural social network:** for exchange of agriculture related information by farmers from different parts of India (or the world). Share information about NREGA, MSP, cost of fertilisers, ...
- **Online rural credit system:** to provide credit to farmers freeing them from money lenders.



Opportunities for Innovative Applications

Rapid development of mobile communication technology and the fast disappearing digital divide.

Online services over mobile phones can now be leveraged in the villages.
Opens up possibilities for new business applications geared towards rural India.

- **Rural social network:** for exchange of agriculture related information by farmers from different parts of India (or the world). Share information about NREGA, MSP, cost of fertilisers, ...
- **Online rural credit system:** to provide credit to farmers freeing them from money lenders.

Research problem: Design and implement comprehensive solutions for these (and other related) applications.



Thank you for your attention!

