On Using Mathematics to Attain Secrecy

Palash Sarkar

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

A Talk to the B. Math Students
Indian Statistical Institute
Bangalore Centre
24^{th} February 2012

Secrecy of Communication

In real life, attaining secrecy of communications is a complex task.

Requires combination of knowledge from various branches of sciences.

- Mathematics and statistics.
- Computer Science.
- Engineering.
- ...

Secrecy of Communication

In real life, attaining secrecy of communications is a complex task.

Requires combination of knowledge from various branches of sciences.

- Mathematics and statistics.
- Computer Science.
- Engineering.
- ...

In this talk, we briefly describe how mathematics can be used to answer the following two questions.

- How to share a secret?
- How to agree upon a secret?

How to share a secret?

Secret Sharing: Motivation

Bank lockers.

- Account holder and bank have separate keys.
- Both keys are required to open a locker.
- 2-out-of-2 sharing.

Secret Sharing: Motivation

Bank lockers.

- Account holder and bank have separate keys.
- Both keys are required to open a locker.
- 2-out-of-2 sharing.

Weapon codes.

- Several persons are given ‘shares’.
- If a certain number of these persons come together, then the actual value can be constructed.
- k-out-of-n sharing.

2-Out-Of-2 Sharing

Secret: an integer $s \in \{0, \ldots, N-1\}$ for some known N.

Share Creation:

- Choose a_0 uniformly at random from $\{0, \ldots, N-1\}$.
- Set $a_1 = s - a_0 \bmod N$.
- The two shares are a_0 and a_1.

Reconstruction: $a_0 + a_1 \bmod N$.

2-Out-Of-2 Sharing

Secret: an integer $s \in \{0, \ldots, N-1\}$ for some known N.

Share Creation:

- Choose a_0 uniformly at random from $\{0, \ldots, N-1\}$.
- Set $a_1 = s - a_0 \bmod N$.
- The two shares are a_0 and a_1.

Reconstruction: $a_0 + a_1 \bmod N$.

Secrecy:

- a_0 is a uniform random value in the range $\{0, \ldots, N-1\}$.
- a_1 is a uniform random value in the range $\{0, \ldots, N-1\}$.
- Individually, neither a_0 nor a_1 reveal any information about s.

2-Out-Of-2 Sharing

Secret: an integer $s \in \{0, \ldots, N-1\}$ for some known N.

Share Creation:

- Choose a_0 uniformly at random from $\{0, \ldots, N-1\}$.
- Set $a_1 = s - a_0 \bmod N$.
- The two shares are a_0 and a_1.

Reconstruction: $a_0 + a_1 \bmod N$.

Secrecy:

- a_0 is a uniform random value in the range $\{0, \ldots, N-1\}$.
- a_1 is a uniform random value in the range $\{0, \ldots, N-1\}$.
- Individually, neither a_0 nor a_1 reveal any information about s.

Easily generalises to k-out-of-k scheme.

Threshold Secret Sharing

- There are n users; each user gets a share.
- If any k users combine their shares, then the secret can be reconstructed.
- If less than k users combine their shares, then no information is revealed about the secret.

Shamir's Secret Sharing

Proposed by Shamir in 1979.

Secret: an integer $s \in \{0, \ldots, p-1\}$ where p is a prime.

Shamir's Secret Sharing

Proposed by Shamir in 1979.

Secret: an integer $s \in \{0, \ldots, p-1\}$ where p is a prime.

Share Creation:

- Set $c_0 = s$; choose $c_1, \ldots, c_{k-1}$ independently and uniformly from $\mathbb{Z}_p$.
- Define $P(x) = c_0 + c_1 x + \cdots + c_{k-1} x^{k-1}$.
- The n shares are $(i, a_i = P(i) \bmod p)$, $1 \leq i \leq n$.

(More generally, one can work with any finite field $\mathbb{F}$.)

Shamir's Secret Sharing (contd.)

Share Reconstruction:

- Suppose shares (i_j, a_{i_j}), $1 \leq j \leq k$ are to be combined.
- This gives rise to the following system of linear equations.

$$\begin{bmatrix} 1 & i_1 & i_1^2 & \cdots & i_1^{k-1} \\ 1 & i_2 & i_2^2 & \cdots & i_2^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & i_k & i_k^2 & \cdots & i_k^{k-1} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{k-1} \end{bmatrix} = \begin{bmatrix} a_{i_1} \\ a_{i_2} \\ \vdots \\ a_{i_k} \end{bmatrix}$$

- The matrix is a Vandermonde matrix and can be inverted to obtain $s = c_0$ and also $c_1, \ldots, c_{k-1}$.
- Alternatively, this can be viewed as a polynomial interpolation problem.

Shamir's Secret Sharing (contd.)

Secrecy.

- If $t < k$ users combine their shares, then we obtain a partial $t \times k$ Vandermonde matrix.
- The rank of this matrix is $t < k$.
- For any value of $s = c_0$, there is a solution to the linear system.
- So, no value can be ruled out for s. In other words, the t shares reveal no information about s.

Secret Sharing: Further Comments

- The access structure considered is called a threshold access structure.
- Shamir's secret sharing scheme essentially uses an error-correcting code called the Reed-Solomon code.
- Any linear error-correcting code can be used to obtain a secret-sharing scheme.
- Allows sharing using more general access structures.
- Secret sharing is one of the basic primitives for constructing other cryptographic schemes such as secure multi-party computation.

How to agree upon a secret?

Agreeing Upon a Secret

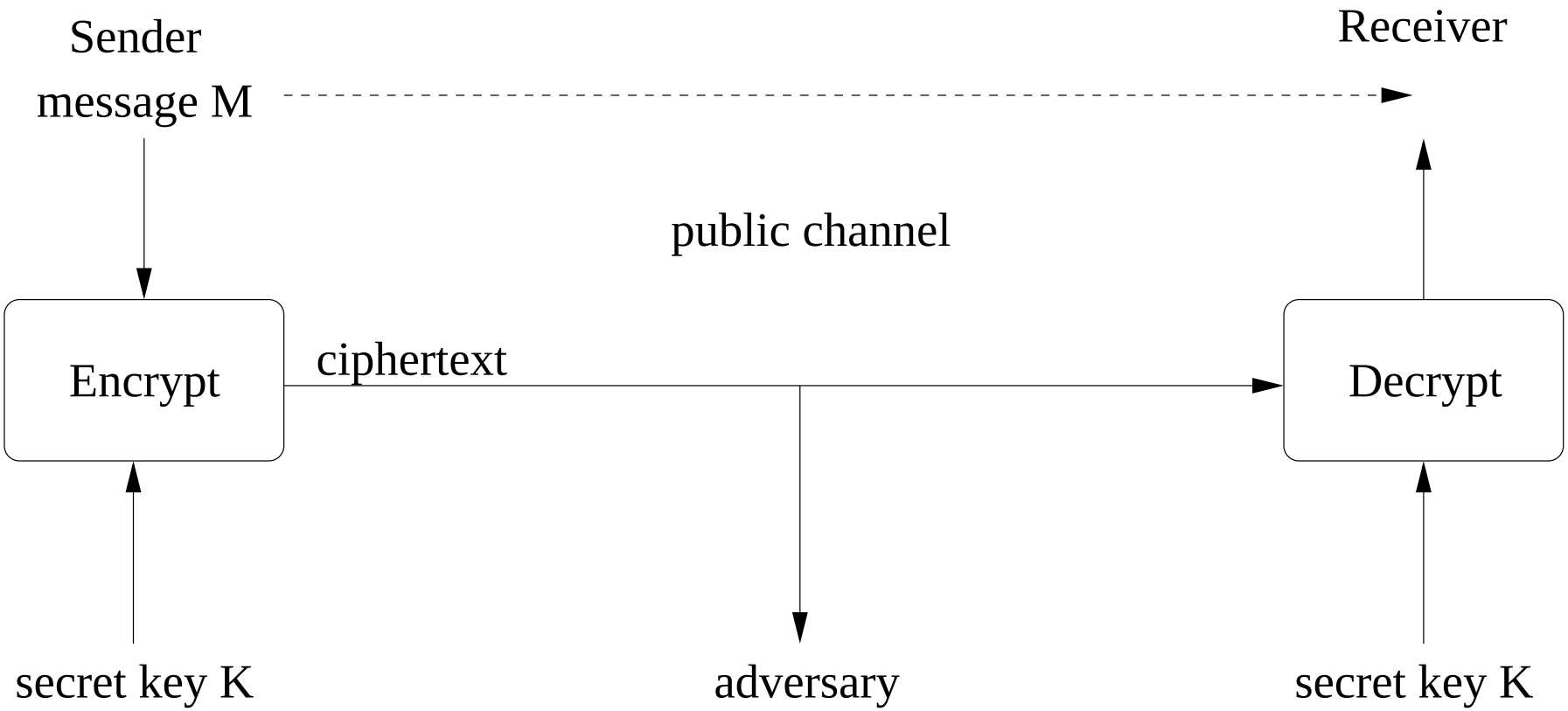
- If two persons are together, then they can agree upon a secret.
- Suppose two persons are geographically apart and can only communicate using a public channel.
- Is it possible for two persons to agree upon a secret through public discussion?

Agreeing Upon a Secret

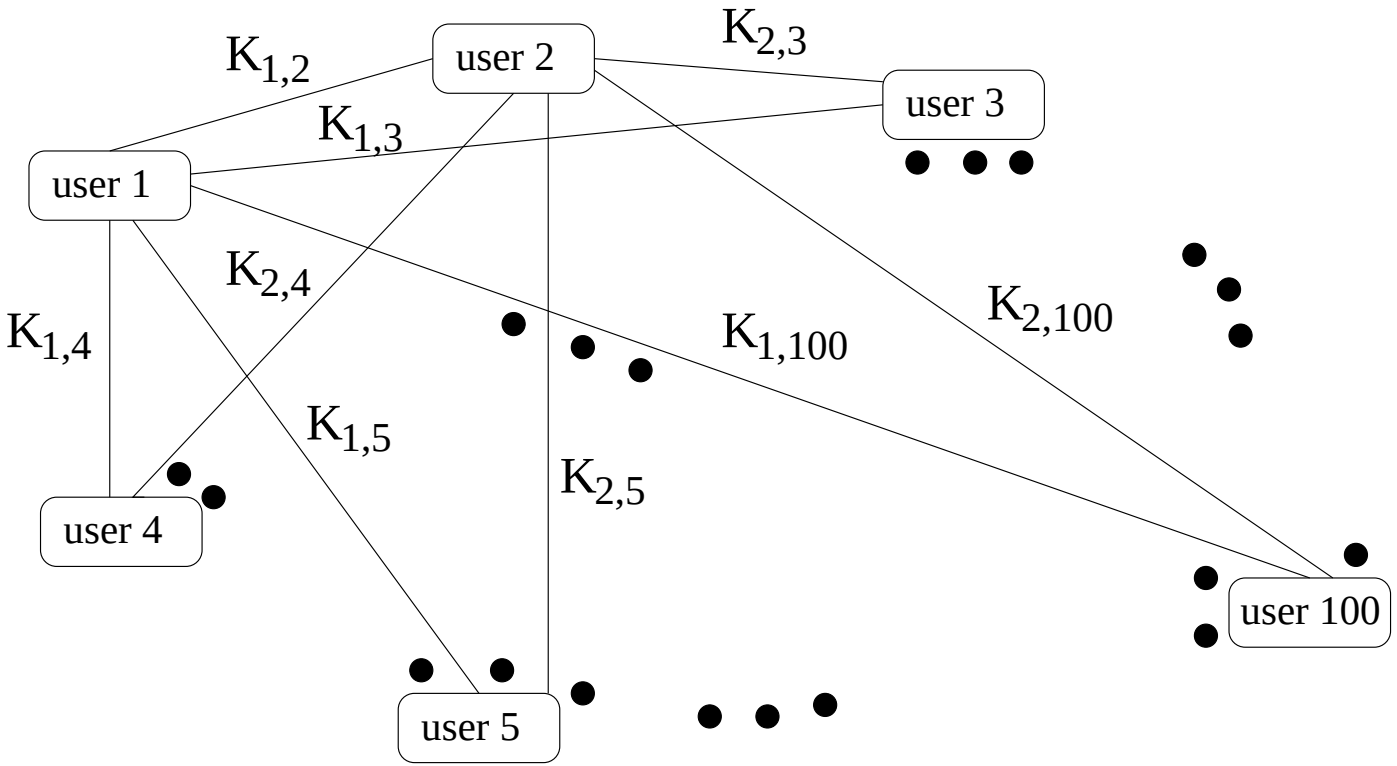
- If two persons are together, then they can agree upon a secret.
- Suppose two persons are geographically apart and can only communicate using a public channel.
- Is it possible for two persons to agree upon a secret through public discussion?

Why is it at all necessary to agree upon a secret?

Conventional Model of Encryption



The Key Management Problem



- There are $\binom{100}{2}$ bi-directional links.
- Each link has an associated secret key.
- Each user has to maintain the secrecy of 99 keys.

Change 100 to larger n to see the immensity of the problem!

Diffie-Hellman Public Key Agreement

How to agree upon a secret through public discussion?

Diffie-Hellman Public Key Agreement

How to agree upon a secret through public discussion?

Cyclic group $G = \{1, g, g^2, \ldots, g^{p-1}\}$

Alice		Bob
1. Choose secret a;		1. Choose secret b;
2. Compute g^a;		2. Compute g^b;
	send g^a →	
	← send g^b	
3. Compute $K=(g^b)^a=g^{ab}$		3. Compute $K=(g^a)^b=g^{ab}$

Computationally Hard Problems

Computational Diffie-Hellman Problem.

Given (g, g^a, g^b) compute g^{ab}.

Discrete Logarithm Problem.

Given $(g, h = g^a)$ compute $a \stackrel{\Delta}{=} \log_g h$.

Computationally Hard Problems

Computational Diffie-Hellman Problem.

Given (g, g^a, g^b) compute g^{ab}.

Discrete Logarithm Problem.

Given $(g, h = g^a)$ compute $a \stackrel{\Delta}{=} \log_g h$.

If DL can be solved, then CDH can be solved
and then DH-KA can be 'broken'.

Computationally Hard Problems

Computational Diffie-Hellman Problem.

Given (g, g^a, g^b) compute g^{ab}.

Discrete Logarithm Problem.

Given $(g, h = g^a)$ compute $a \stackrel{\Delta}{=} \log_g h$.

If DL can be solved, then CDH can be solved
and then DH-KA can be 'broken'.

Necessary criterion for security: Choose the group order p to be large enough so that solving DLP becomes infeasible.

Computationally Hard Problems

Computational Diffie-Hellman Problem.

$$\text{Given } (g, g^a, g^b) \text{ compute } g^{ab}.$$

Discrete Logarithm Problem.

$$\text{Given } (g, h = g^a) \text{ compute } a \stackrel{\Delta}{=} \log_g h.$$

If DL can be solved, then CDH can be solved
and then DH-KA can be 'broken'.

Necessary criterion for security: Choose the group order p to be large enough so that solving DLP becomes infeasible.

Efficiency issue: Working with a larger group will slow down the computations.

Suitable Groups

- **A suitable subgroup of the multiplicative group of a finite field.**
  - Binary, i.e., $GF(2^n)$ or large characteristics, i.e., $GF(p)$.
  - Sub-exponential algorithm for discrete log problem.

$$\exp\left((\log \#\mathbb{F})^c (\log\log \#\mathbb{F})^{1-c}\right).$$

Suitable Groups

- **A suitable subgroup of the multiplicative group of a finite field.**
  - Binary, i.e., $GF(2^n)$ or large characteristics, i.e., $GF(p)$.
  - Sub-exponential algorithm for discrete log problem.

$$\exp\left((\log \#\mathbb{F})^c (\log\log \#\mathbb{F})^{1-c}\right).$$

- **Group of points on an elliptic curve over a finite field.**
  $\mathrm{char}(\mathbb{F}) \neq 2, 3$: simplied Weierstraß form:

$$y^2 = x^3 + ax + b \qquad (*)$$

  $a, b \in \mathbb{F}$ and $4a^3 + 27b^2 \neq 0$.
  - Points (x, y) satisfying $(*)$ form a group under a suitably defined addition law.
  - Cryptography is done over a suitable prime order subgroup.
  - No known sub-exponential algorithm for the discrete log problem.
  - Smaller key sizes and faster encryption/decryption algorithms.

Group Key Agreement: Burmester-Desmedt (1994)

Suppose there are n users $U_1, \ldots, U_n$:

Group Key Agreement: Burmester-Desmedt (1994)

Suppose there are n users $U_1, \ldots, U_n$:

- **Round 1:**
  - U_i chooses a uniform random r_i from $\{0, \ldots, p-1\}$.
  - U_i computes $z_i = g^{r_i}$ and broadcasts this value.
- **Round 2:**
  U_i computes $X_i = (z_{i+1}/z_{i-1})^{r_i}$ and broadcasts this value.
- **Key computation:**
  Each user computes $K_i = (z_{i-1})^{nr_i} X_i^{n-1} X_{i+1}^{n-2} \cdots X_{i-2}$.

Group Key Agreement: Burmester-Desmedt (1994)

Suppose there are n users $U_1, \ldots, U_n$:

- **Round 1:**
  - U_i chooses a uniform random r_i from $\{0, \ldots, p-1\}$.
  - U_i computes $z_i = g^{r_i}$ and broadcasts this value.
- **Round 2:**
  U_i computes $X_i = (z_{i+1}/z_{i-1})^{r_i}$ and broadcasts this value.
- **Key computation:**
  Each user computes $K_i = (z_{i-1})^{nr_i} X_i^{n-1} X_{i+1}^{n-2} \cdots X_{i-2}$.

Let $A_i \stackrel{\Delta}{=} z_i^{r_{i+1}} = g^{r_i r_{i+1}} = z_{i+1}^{r_i}$.

Then $A_{i-1} = z_{i-1}^{r_i}$; $A_i = z_{i-1}^{r_i} X_i$; $A_{i+1} = z_{i-1}^{r_i} X_i X_{i+1}$; ....

$$K_i = A_{i-1} A_i A_{i+1} \cdots A_{i-2} = g^{r_1 r_2 + r_2 r_3 + \cdots + r_n r_1}.$$

Summary

- A brief idea of secret sharing.
- A brief idea of public key agreement.

Summary

- A brief idea of secret sharing.
- A brief idea of public key agreement.

Cryptology offers many more interesting problems!

Thank you for your attention!