

# Hauptseminar: Logjam

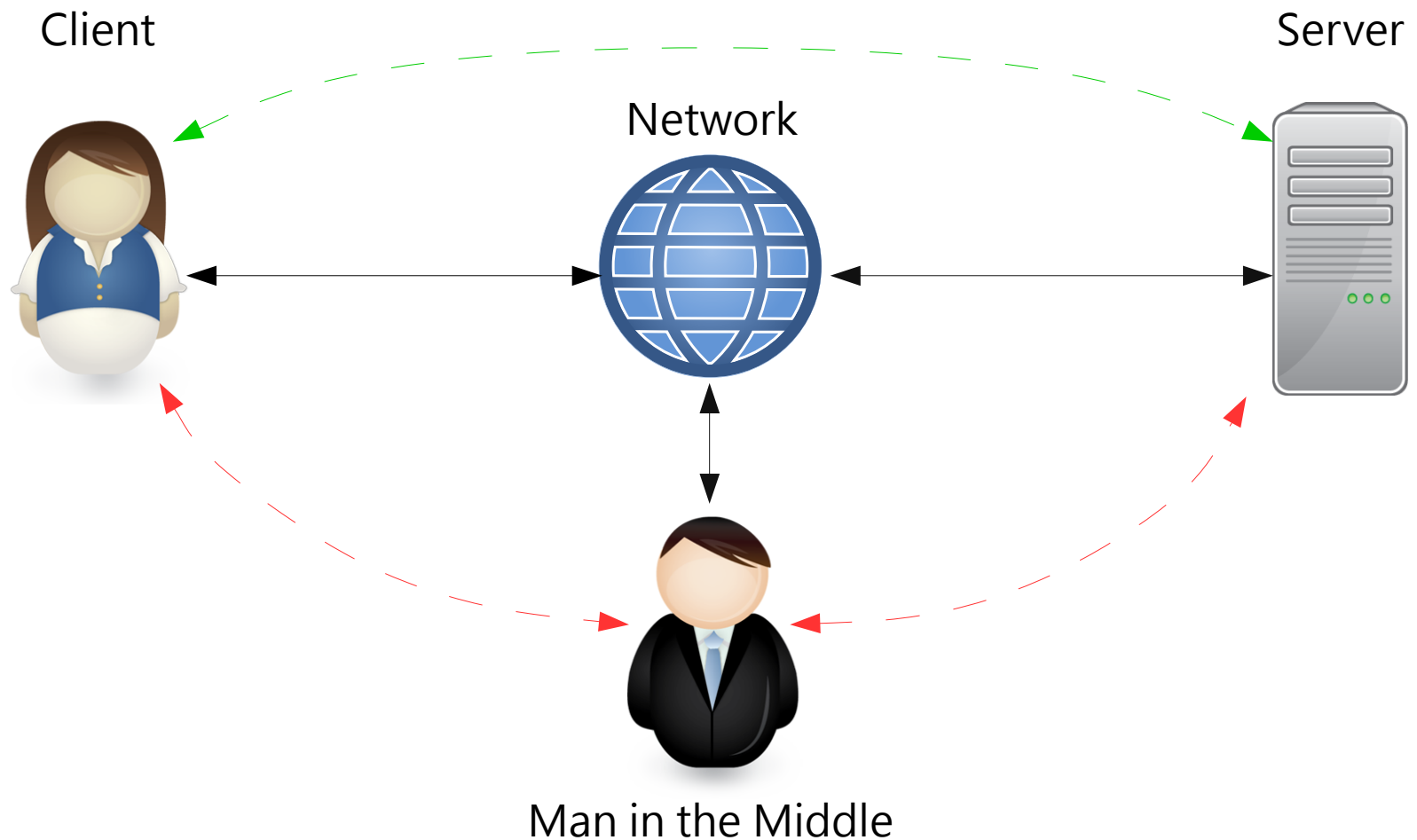
by Li Yang Wu

# Content

- Logjam
- Diffie-Hellman Key Exchange
- Number Field Sieve
- Transport Layer Security Handshake
- Logjam Summary
- Breaking 1024 bit Groups

# Logjam

- The situation:

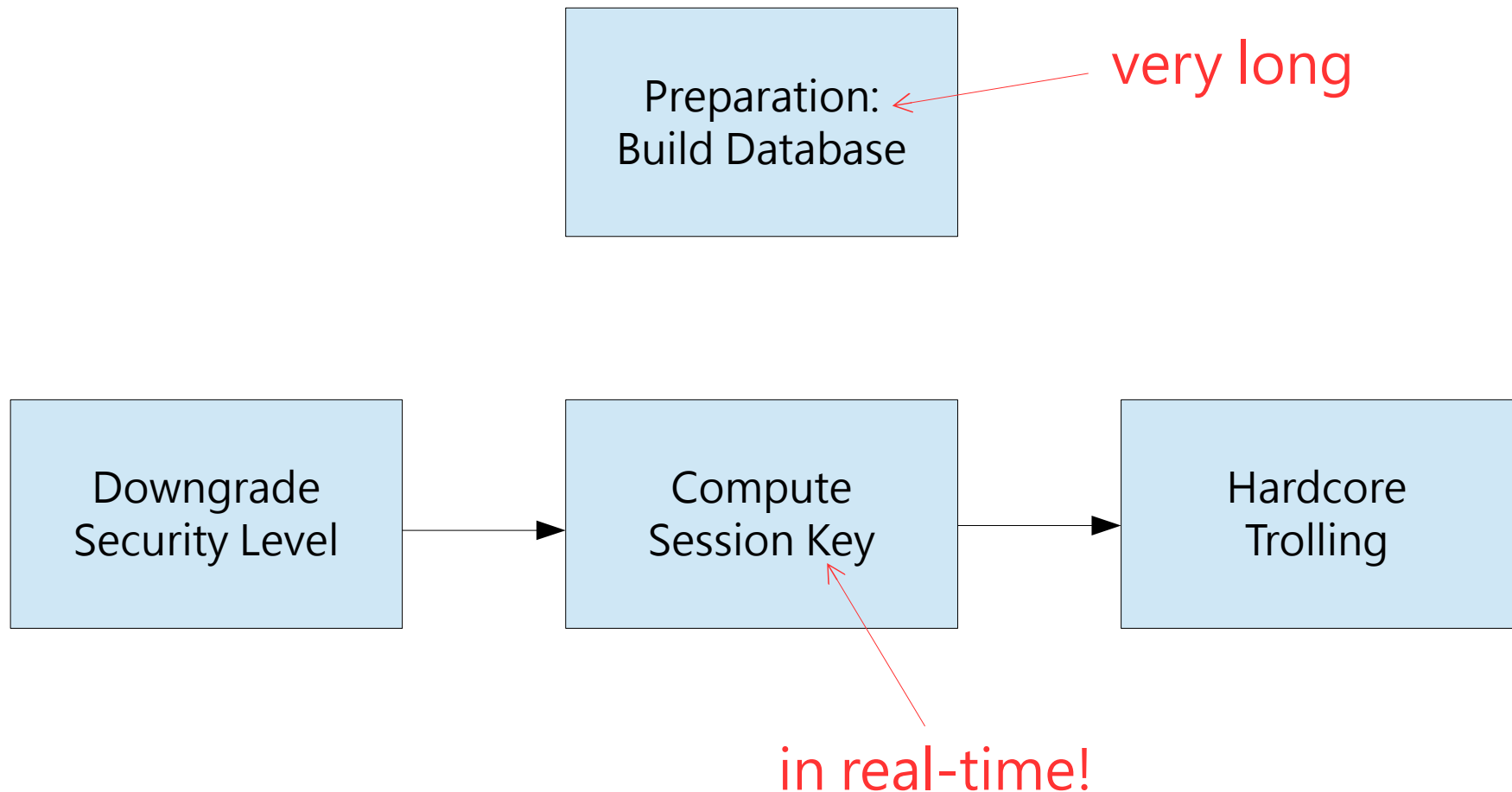


# Logjam

- Attack on network security protocol
  - Secure client-server communication
- Exploits TLS 1.2 handshake flaw
- Downgrade security level in Diffie-Hellman
- In theorie: easy to avoid
- In practice: high success

# Logjam

- Approach:



# Content

- Logjam
- Diffie-Hellman Key Exchange
- Number Field Sieve
- Transport Layer Security Handshake
- Logjam Summary
- Breaking 1024 bit Groups

# DH Key Exchange

- Given:
  - Communication partners A and B
  - Insecure communication channel
  - Message space
- Determine:
  - Public key cryptosystem
  - Key space
  - ... with exponential cipher-cryptanalyst ratio

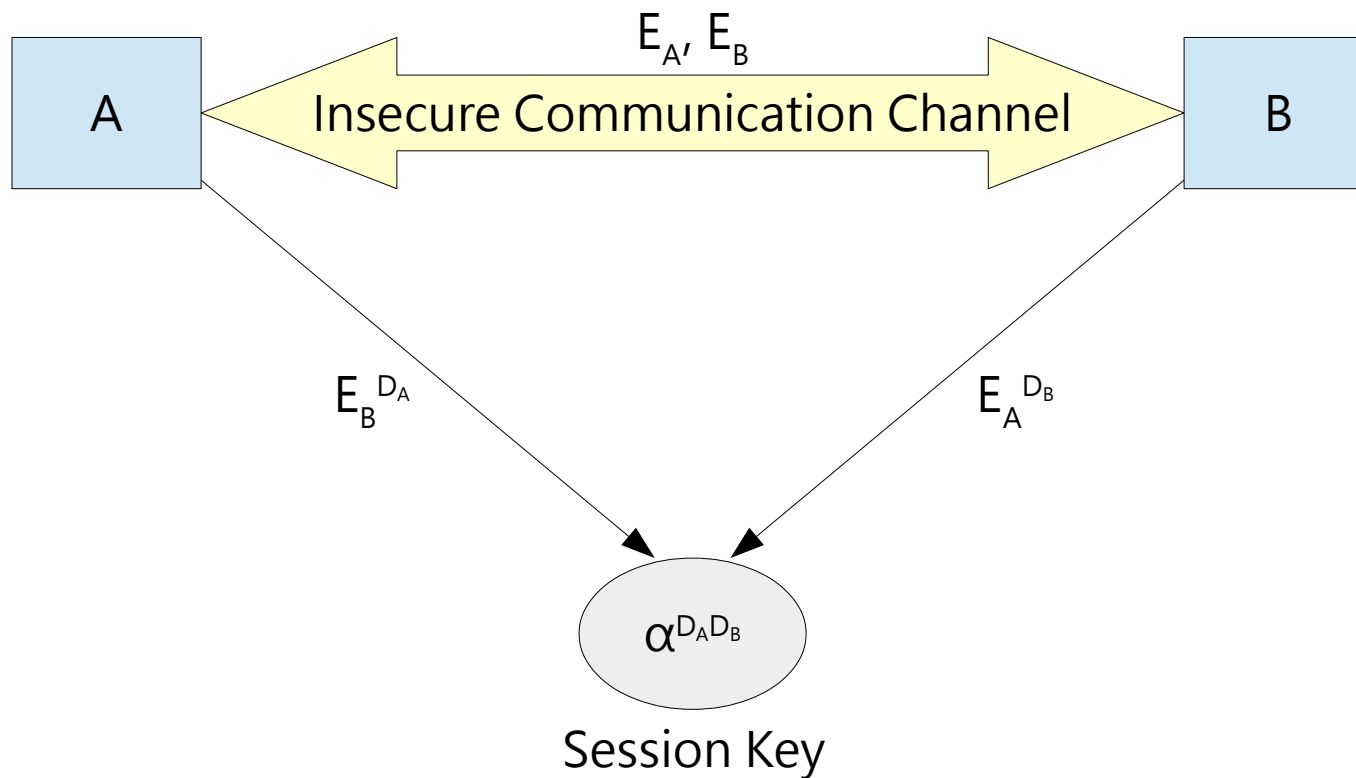
# DH Key Exchange

- Define key space:
  - Choose prime  $q$
  - Define number field  $GF(q) = \mathbb{Z}/q\mathbb{Z}$
  - Choose basis  $\alpha$  in  $GF(q)$
- Draw keys:
  - Choose private key  $D$  in  $GF(q)$
  - Calculate public key  $E = \alpha^D \bmod q$
- We have:  $D_{A'}, D_{B'}, E_{A'}, E_B$



# DH Key Exchange

- Session key:



Remember:  $E = \alpha^D \bmod q$

# DH Key Exchange

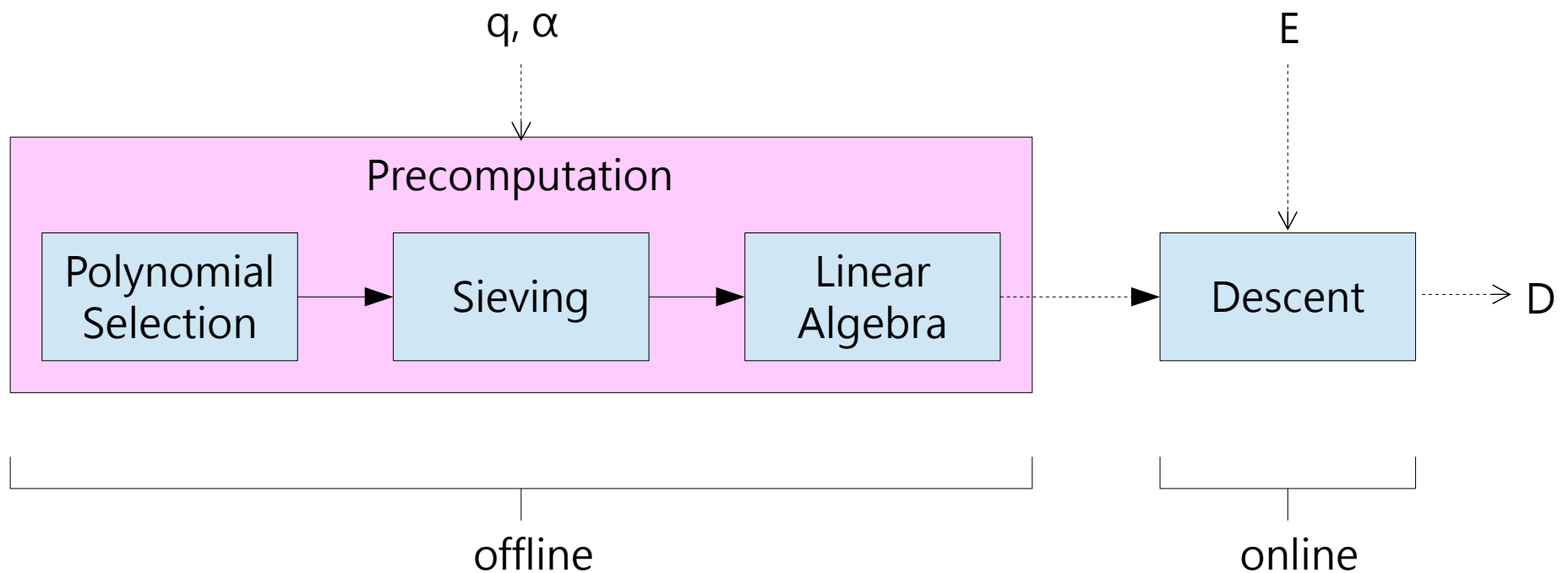
- Cryptanalyst:
  - Knowledge:  $\alpha, q, E_A, E_B$
  - Objective:  $D_A$  or  $D_B$
  - Calculate Logarithm:  $D = \log_{\alpha} E \bmod q$
  - Cost:  $O(\sqrt{q})$
  - Cost of taking  $\alpha^{D_A D_B} \bmod q$  is only  $O(\log(q))$
  - $\Rightarrow$  **Exponential** cipher-cryptanalyst ratio

# Content

- Logjam
- Diffie-Hellman Key Exchange
- Number Field Sieve
- Transport Layer Security Handshake
- Logjam Summary
- Breaking 1024 bit Groups

# Number Field Sieve

- Approach:



# Number Field Sieve

- Polynomial Selection:
  - Find polynomial  $f$  and choose  $m$  s.t.  $f(m) \equiv 0 \pmod{q}$
  - Based on  $f$ , find a ring of integers  $O$  and homomorphism s.t.  $\varphi : \mathbb{Z}[\gamma] \rightarrow \mathbb{Z}/q\mathbb{Z}$ , where  $\gamma$  is some root of  $f$
- Benefit: Express knowledge about logs of factors of  $\alpha$  with linear equations.

# Number Field Sieve

- Sieving:
  - Define the set of "good" prime ideals  $B$  in  $O$
  - Sieve through pairs of integers  $(c,d)$  that are related to elements in  $B$
  - Form matrices from these relations
  - Modify matrices to express only information about log factors of  $\alpha$
- Output: Some matrices  $A_i$

# Number Field Sieve

- Linear Algebra:
  - Take matrices  $A_i$
  - Compute rank  $r$  and extract matrices  $A_i'$  with sizes of its ranks
  - Find set  $P$  of primes  $p_i$  with bounded
  - Compute  $\det(A) \bmod p$  for each  $p_i$  in  $P$
  - Find relations between the  $(r+1)^{\text{th}}$  row and  $A_i'$
  - Calculate logs of prime factors of  $\alpha$

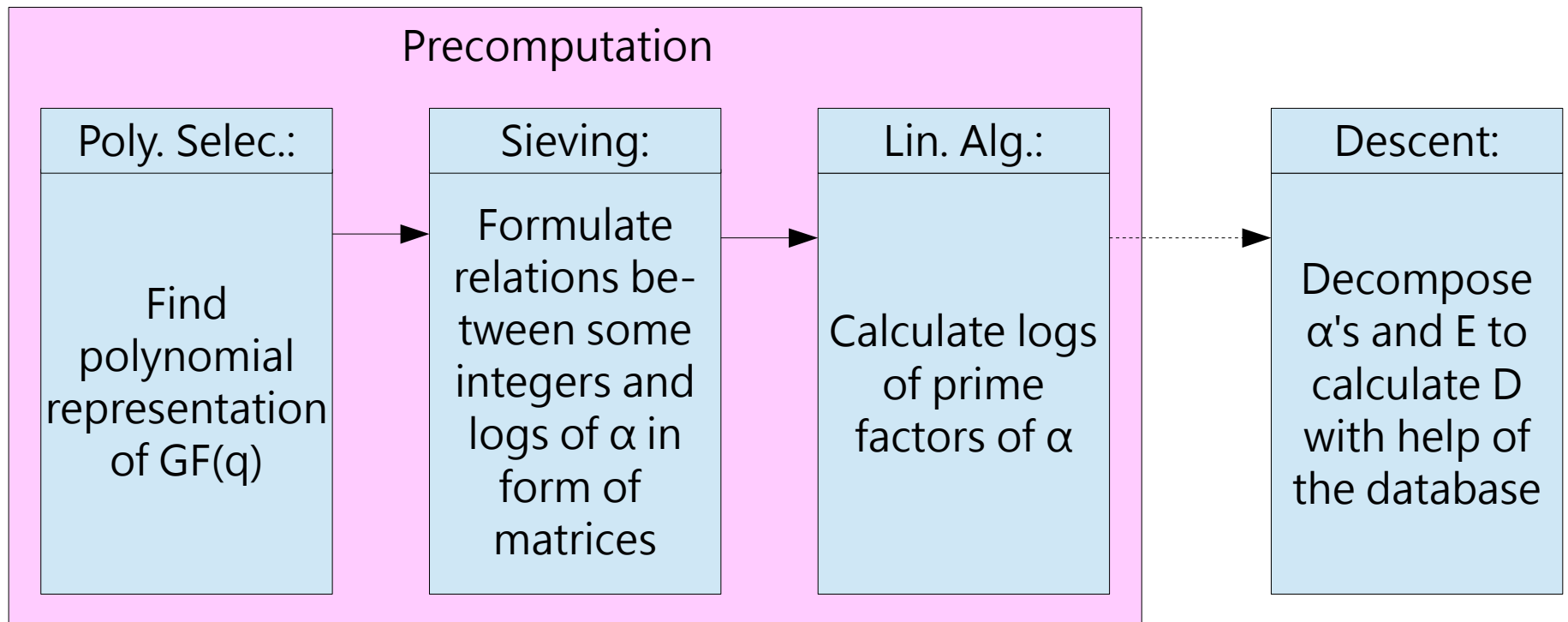
# Number Field Sieve

- Descent:
  - Find  $l$  s.t.  $\alpha^l E \equiv p_1 p_2 \dots p_t \pmod{q}$ , for small  $p_i$ 's
  - Find logs of  $p_i$ 's with database
  - Compute  $D$  from these logs



# Number Field Sieve

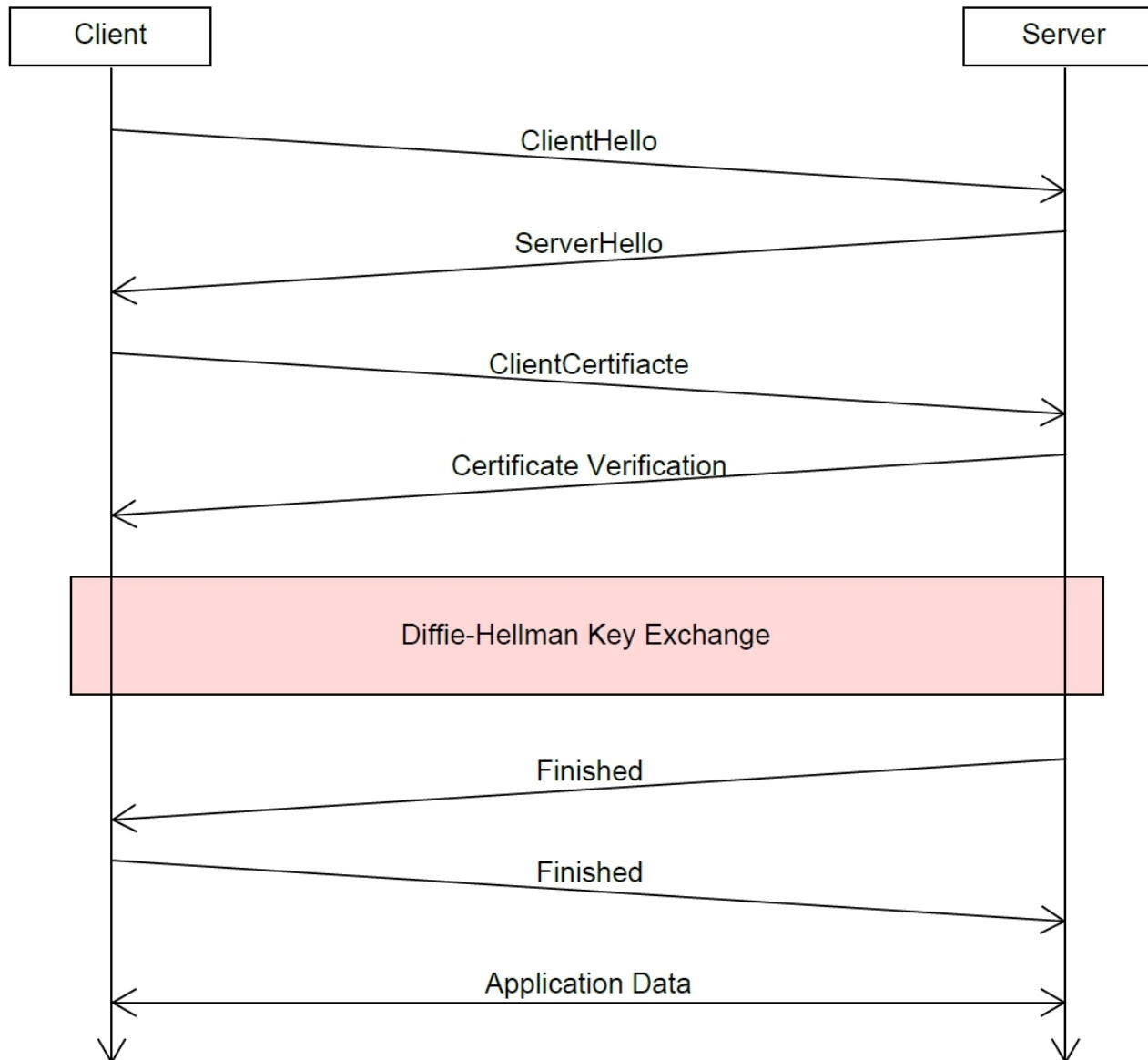
- Refined Approach:



# Content

- Logjam
- Diffie-Hellman Key Exchange
- Number Field Sieve
- Transport Layer Security Handshake
- Logjam Summary
- Breaking 1024 bit Groups

# TLS Handshake



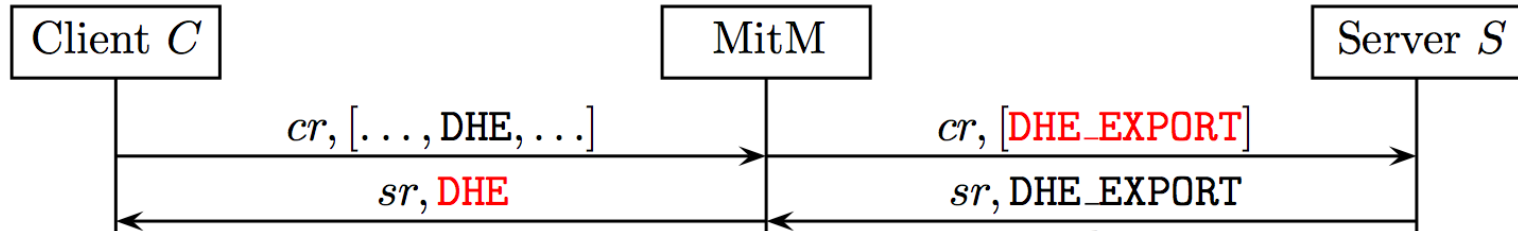
# Content

- Logjam
- Diffie-Hellman Key Exchange
- Number Field Sieve
- Transport Layer Security Handshake
- Logjam Summary
- Breaking 1024 bit Groups

# Logjam Summary

- Preparation:
  - Use the most common 512 Apache group for DH
  - Do the precomputation according to NFS
- Now our database is ready

# Logjam Summary



# Logjam Summary

- Success Rate:
  - 8.4% top 1M Alexa sites
  - 3.4% sites with browser-trusted certificates

# Content

- Logjam
- Diffie-Hellman Key Exchange
- Number Field Sieve
- Transport Layer Security Handshake
- Logjam Summary
- Weak DH Parameters
- Breaking 1024 bit Groups



# Weak DH Parameters

- Use Pollard's lamda method and Pohlig-Hellman decomposition for an improved log calculation if  $E$  is chosen small and  $q$  is not chosen "safe".
  - Pollard's lambda method calculates logs efficiently, if it is known to lie in a fixed bound  $\{b, \dots, b+w\}$
  - Pohlig-Hellman decomposition extracts information about logs given some prime factors of  $q-1$

# Weak DH Parameters

- Improved attack:
  - Decompose  $q-1$  in prime factors
  - Extract information of the log from factors for which the log is feasible to compute (Pohlig-Hellman)
  - Express the missing information as a new log problem with fixed bounds.
  - Solve with Pollard's lambda method

# Content

- Logjam
- Diffie-Hellman Key Exchange
- Number Field Sieve
- Transport Layer Security Handshake
- Logjam Summary
- Breaking 1024 bit Groups

# Breaking 1024 bit Groups

- Only a cost estimation
- Motivation: Edward Snowden leaks
  - Assertion: NSA decrypts all communication
- Assumptions:
  - Optimistic cost extrapolation of recent records in factorization and log computation
  - Existence of specialized hardware for certain tasks

# Breaking 1024 bit Groups

- Result:
  - Total cost slightly over \$11B
  - Budget for Consolidated Cryptographic Program plus some additional investments: over \$11B