

Constant Round Authenticated Group Key Agreement

Emmanuel BRESSON
CELAR, France

Dario CATALANO
ENS, France

PKC 2004 — March 1-4, Singapore, SG

1

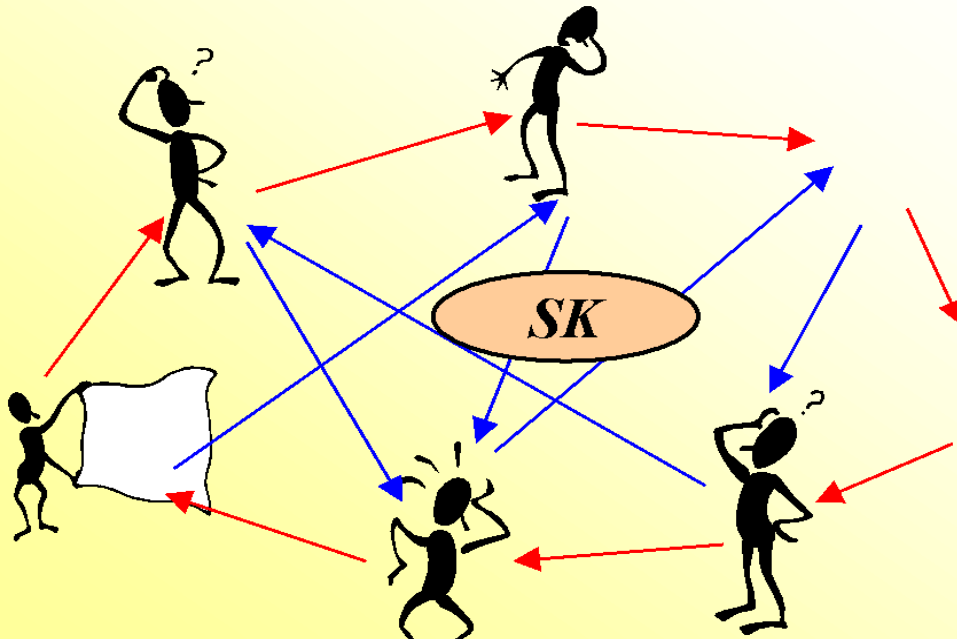
Outline

- Introduction
 - Security definition
 - Efficiency issues
- Proposed scheme
 - Description of the scheme
 - Security theorem
- Conclusion

PKC 2004 — March 1-4, Singapore, SG

2

Group Key Agreement



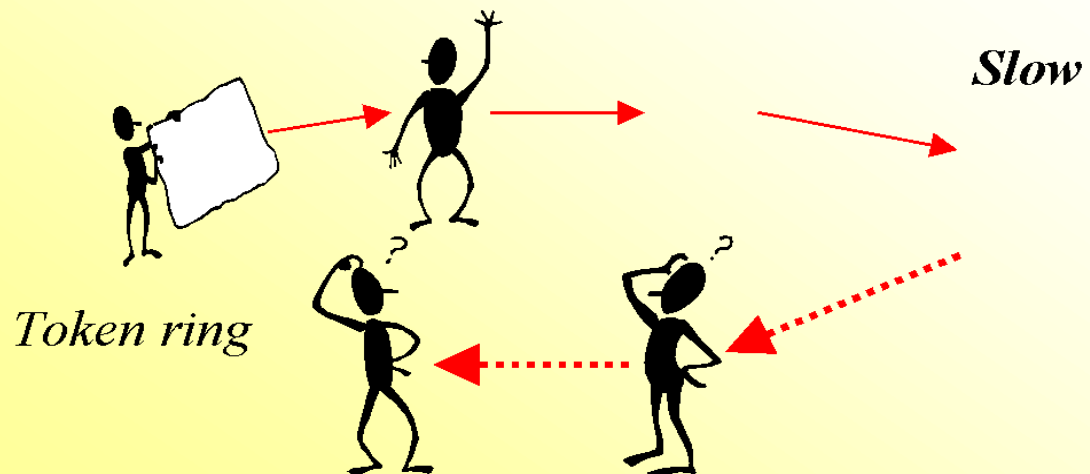
PKC 2004 — March 1-4, Singapore, SG

3

Communications

■ Efficiency

- Considering a network with one single low connection



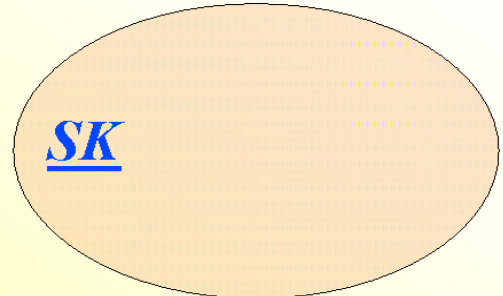
PKC 2004 — March 1-4, Singapore, SG

4

Security Goals

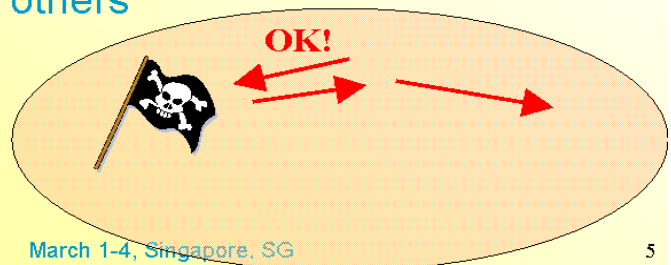
■ Privacy

- nobody outside the group should learn the key



■ Authentication

- nobody should fool the others
- everybody is sure to obtain the right info from the right partner



Other Issues

■ Provable security issues:

- To be based on alternative schemes than DH Key Exchange
- A line of basic research
- Both theoretical ...
 - Security and complexity point of view
- ... and practical importance
 - Efficiency and implementation issues

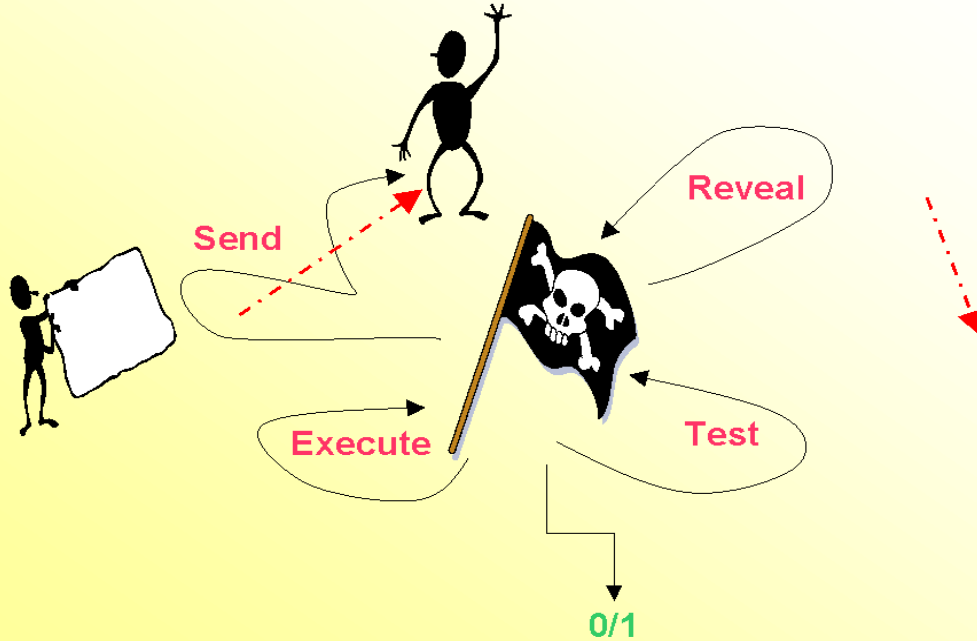
Our Results

- An alternative solution to DH schemes
- An efficient protocol running in constant rounds
- A provably secure scheme (in the standard model)

Players and Network

- Players have certified public keys
 - A trusted PKI is assumed
 - Messages are authenticated via signatures
- Network is under adversary's control
 - Modification, delay, insertion of messages
 - Players are available through queries made by the adversary

Security Model



PKC 2004 — March 1-4, Singapore, SG

9

Security Notions

- **Completeness**
 - If no adversary is active, the protocol establishes a common key for all P_i
- **Semantic security of the key**
 - The session key should be undistinguishable from a random string
- **Authentication**
 - A key confirmatory mechanism
- **Perfect-forward secrecy**
 - Security of past session keys even if corruption

PKC 2004 — March 1-4, Singapore, SG

10

Our Main Idea

- Each player sends a contribution nonce
 - A rushing player might wait for other contributions before choosing its own
- Use polynomial secret sharings to distribute information-theoretically hidden masks
 - Separate in two rounds
 - Contributions are sent before getting the masks
 - Masks are sent and interpolated in the second round only
 - A “so far, so good” behavior
 - Protects against “honest-but-curious” only

The Proposed Scheme

- Round 1
 - Each P_i chooses a contribution a_i
 - Each P_i chooses a $(n-1)$ -degree polynomial f_i such that $f_i(0)=r_i$: player's randomizer
 - Each P_i sends $f_i(j)$ and an encryption of a_i to P_j
- Round 2
 - Each P_i decrypts the contributions to get a_i
 - Each P_i computes its share of the global polynomial $f=\sum_k f_k$ and sends it (signed)
- Round 3: session key is defined = $g^{f(0)}\prod a_k$

The Scheme

Round 1
Round 2

Compute $f(1)$



Receive all

$f_i(1), i > 1$

Sends $EIG(a_i)$ + shares of $f_1(0)$, for $i > 1$

$f(1)$ shares $f(0)$

$$sk = g^{f(0)} \prod a_i$$

The Polynomial Shares

Received by P_i

Sent by P_i

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(\dots)$	$f_1(n)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(\dots)$	$f_2(n)$
$f_i(1)$	$f_i(2)$	$f_i(\dots)$	$f_i(\dots)$	$f_i(n)$
....
$f_n(1)$	$f_n(2)$	$f_n(\dots)$	$f_n(\dots)$	$f_n(n)$

$f(1)$ $f(2)$ $f(\dots)$ $f(\dots)$ $f(n)$

Security Theorem

- The scheme establishes a semantically secure session key, provided the underlying encryption scheme is so
- The session key remains uniformly distributed in the key space, as soon as one player chooses its nonces uniformly
- Authentication can be done using PRFs

Efficiency of the Scheme

- Basic version
 - Each player sends (with signatures)
 - n ciphertexts
 - $n+1$ polynomial shares
 - Computations
 - $2n+2$ exponentiations
- With pre-processing
 - All exponentiations in the first round can be precomputed

Generalization

- Security is still based on Diffie-Hellman...
 - El Gamal has nice homomorphic properties
=> Increases the efficiency
- Can be based on more general complexity assumptions
 - Any semantically secure encryption scheme can be used
 - ... but less efficient construction

Conclusion

- A new efficient scheme
 - Constant number of rounds
 - Provably secure
 - Without Random Oracle (or for confirmation)
- Can be based on more general assumptions
 - Work in progress
 - Soon available on
<http://www.di.ens.fr/~{bresson,catalano}>