Towards formal analysis of key control in group key agreement protocols

Anshu Yadav and Anish Mathuria

DA-IICT, Gandhinagar

Outline

- Burmester-Desmedt key agreement
  - Pieprzyk-Wang attack
- Delicata-Schneider (DS) proof model [FAST'05], [Int. J. Inf. Secur. '07]
- Using DS model to find/model key control attacks

Group key agreement

- Basic techniques
  - 2-party Diffie-Hellman
  - Public but authentic channels
- Contributory property
  - the final value of the key is dependent on the ephemeral inputs of all parties

Key Control Attacks: Pieprzyk-Wang'04

- Insiders: Actual members of the group which are agreeing on a key

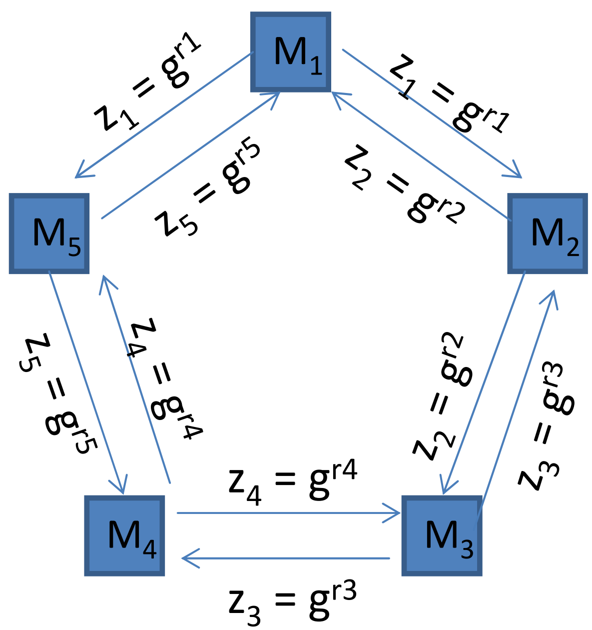
- Two types of attack
  - Strong key control: the malicious insiders force the key to be a pre-defined value of their choosing
  - Selective key control: the malicious insiders remove the *contributions* of some, but not all, honest parties

Burmester-Desmedt Protocol
[Eurocrypt'94]

Suppose n members, M_1, M_2, …, M_n, are arranged in a ring. Every member M_i chooses its private ephemeral value r_i randomly.

Phase 1 uses only communication between adjacent members

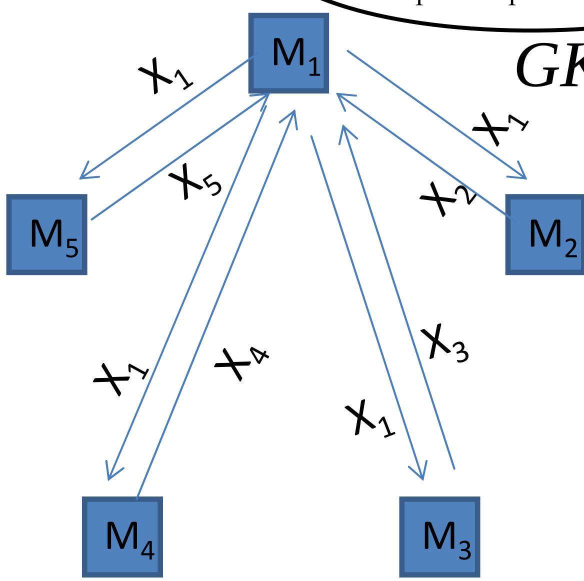
Example:



Phase 2 uses broadcast communications

Example (contd.):

$$K_1^R = z_2^{r_1}; \quad K_1^L = z_5^{r_1}$$
$$X_1 = K_1^R / K_1^L$$



$$GK_1 = (K_1^L)^5 X_1^4 X_2^3 X_3^2 X_4$$
$$= (K_1^L)^5 \left(\frac{K_1^R}{K_1^L}\right)^4 \left(\frac{K_2^R}{K_2^L}\right)^3 \left(\frac{K_3^R}{K_3^L}\right)^2 \left(\frac{K_4^R}{K_4^L}\right)$$
$$= (K_1^L)(K_2^L)(K_3^L)(K_4^L)(K_5^L)$$
$$= g^{r_5 r_1 + r_1 r_2 + r_2 r_3 + r_3 r_4 + r_4 r_5}$$

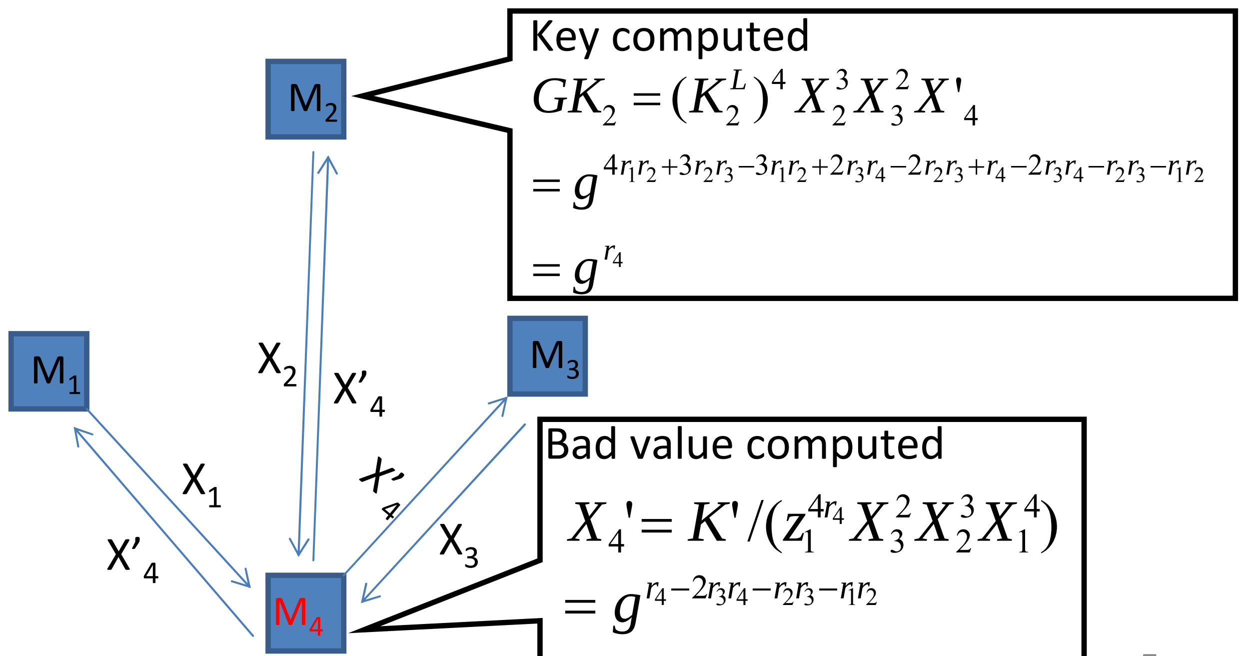
$$K_i^R = z_{i+1}^{r_i}; \quad K_i^L = z_{i-1}^{r_i}$$
$$X_i = K_i^R / K_i^L$$

$$GK_i = (K_i^L)^5 X_i^4 X_{i+1}^3 X_{i+2}^2 X_{i+3}$$

Pieprzyk-Wang Attack: Strong Key Control

Assume M_4 is dishonest and M_2 is the intended victim.
Goal: Fix the key computed by M_2 to be the desired value $K' = g^{r4}$.

M_4 broadcasts a corrupted message derived from other received messages



Attacker model

- Initial knowledge of adversary modeled using two sets

  Set E: $x \in E \Rightarrow$ attacker knows x

  Set P: $y \in P \Rightarrow$ attacker knows g^y, but not y

- Attacker deduction
  - Given $m_1, m_2 \in P$, add m_1+m_2 to P
  - Given $m \in P$ and $n \in E$, add mn to P and (mn^{-1}) to P
  - Given $m \in P$, add $(-m)$ to P

Message-template example

- E = {x, y}; P = {1, a, b}. Note: '1' is identity element

- Consider how the value $g^{(2+a-b)xy+(1+a)xy^2}$ can be expressed. Let

  F = {{x→1, y→1}, {x→1, y→2}}

  h({x→1, y→1}) = {1 →2, a →1, b→-1}

  h({x→1, y→2}) = {1 →1, a →1, b→0}

- Then

$$v(F,h) = \sum_{f \in F} \left(\sum_{p \in P} h_{f,p} \cdot p \right) \left(\prod_{e \in E} e^{f_e} \right)$$

$$= (2 + a - b)xy + (1 + a)xy^2$$

Proving secrecy

- The message-template v(F, h) represents any message generable by an attacker

$$v(F,h) = \sum_{f \in F} \left(\sum_{p \in P} h_{f,p} \cdot p \right) \left(\prod_{e \in E} e^{f_e} \right)$$

- A value m is realisable if there exists functions F and h such that v(F, h) = m

Using DS to find Pieprzyk-Wang attack

- We consider whether there exist realisable values z_1 and z_2 such that

$$(K_2^L)^4 X_2^3 X_3^2 X'_4 = g^{r1r2+r2r3+2r3r4+z1} = g^{z2}$$

- For secrecy to fail, the following equality must hold

$$r_1r_2 + r_2r_3 + 2r_3r_4 + z_1 = z_2$$

- $z_1 = v(F_1, h_1)$ is defined over
  $P_1 = \{1, r_1, r_2, r_3, x_1, x_2, x_3\}$, $E_1 = \{r_4\}$ $(X_i = g^{x_i})$
  $F_1 = \{f_{11}, f_{12}\}$; $f_{11} = \{r_4 \rightarrow p_1\}$, $f_{12} = \{r_4 \rightarrow s_1\}$
  $h_1(f_{11}) = \{1 \rightarrow n_0, r_1 \rightarrow n_1, r_2 \rightarrow n_2, r_3 \rightarrow n_3, x_1 \rightarrow n_4, x_2 \rightarrow n_5, x_3 \rightarrow n_6\}$
  $h_1(f_{12}) = \{1 \rightarrow l_0, r_1 \rightarrow l_1, r_2 \rightarrow l_2, r_3 \rightarrow l_3, x_1 \rightarrow l_4, x_2 \rightarrow l_5, x_3 \rightarrow l_6\}$
  $\mathbf{z_1} = (n_0 + n_1r_1 + n_2r_2 + n_3r_3 + n_4x_1 + n_5x_2 + n_6x_3)r_4^{p1} + (l_0 + l_1r_1 + l_2r_2 + l_3r_3 + l_4x_1 + l_5x_2 + l_6x_3)r_4^{s1}$

Using DS to find Pieprzyk-Wang attack

- $z_2 = v(F_2, h_2)$ is defined over
  $P_2 = \{1\}$, $E_2 = \{r_4\}$
  $F_2 = \{f_{21}\}$; $f_{21} = \{r_4 \rightarrow q_1\}$; $h_2(f_{21}) = \{1 \rightarrow m_0\}$
  $z_2 = m_0 r_4^{q1}$
- $r_1r_2 + r_2r_3 + 2r_3r_4 + (n_0 + n_1r_1 + n_2r_2 + n_3r_3 + n_4x_1 + n_5x_2 + n_6x_3)r_4^{p1} + (l_0 + l_1r_1 + l_2r_2 + l_3r_3 + l_4x_1 + l_5x_2 + l_6x_3)r_4^{s1} = m_0r_4^{q1}$
- Solution:
  Putting $x_1 = r_1r_2 - r_1r_4$; $x_2 = r_2r_3 - r_1r_2$; $x_3 = r_3r_4 - r_2r_3$
  and then solving
  $n_0 = p_1 = m_0 = q_1 = 1$; $n_1 = -4$; $l_4 = -4$; $l_5 = -3$; $l_6 = -2$; rest are 0.
- $z_1 = r_4 - 4r_1r_4 - 2x_3 - 3x_2 - 4x_1$ and $z_2 = r_4$
- This gives $X'_4 = g^{r4}/(z_1^{4r_4}X_3^2X_2^3X_1^4)$ and the resulting key as g^{r4}

Dutta-Barua (DB) Protocol
[IEEE Trans. Inf. Theory, 08]

- The final key is the same as BD protocol but the key computation is different
- Session key = $K_1^R K_2^R \ldots K_n^R = g^{(r_1 r_2 + r_2 r_3 + r_3 r_4 + \cdots r_n r_1)}$

$$K_{i+1}^R = K_i^R X_{i+1}$$

$$K_{i+2}^R = K_{i+1}^R X_{i+2}$$

$$\vdots$$

$$K_{n-1}^R = K_{n-2}^R X_{n-1}$$

$$K_n^R = K_{n-1}^R X_n$$

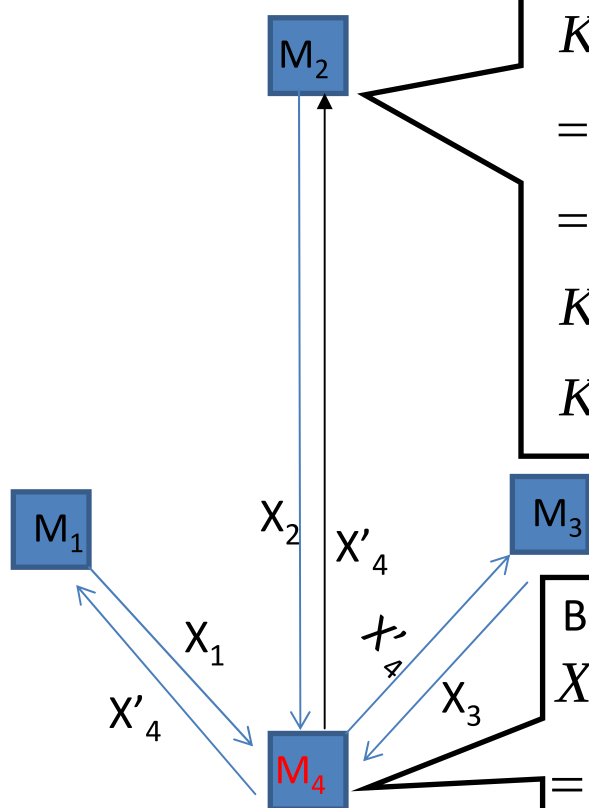
$$K_1^R = K_n^R X_1$$

$$\vdots$$

$$K_{i-1}^R = K_{i-2}^R X_{i-1}$$

- Additional step:

  M_i checks if $K_{i-1}^R = K_i^L$ to detect presence of dishonest insider
- Example: M_4 sends bad value X'_4 to M_2



$$K_1^R = K_2^R X_3 X'_4 X_1$$
$$= g^{r_2r_3+r_3r_4-r_2r_3+(r_4-2r_3r_4-r_2r_3-r_1r_2)+r_1r_2-r_4r_1}$$
$$= g^{r_4-r_3r_4+r_2r_3-r_4r_1}$$
$$K_2^L = g^{r_1r_2}$$
$K_2^L \neq K_1^R$ So M_2 will abort

Bad value computed:
$$X_4' = K'/(z_1^{4r_4} X_3^2 X_2^3 X_1^4)$$
$$= g^{r_4-2r_3r_4-r_2r_3-r_1r_2}$$

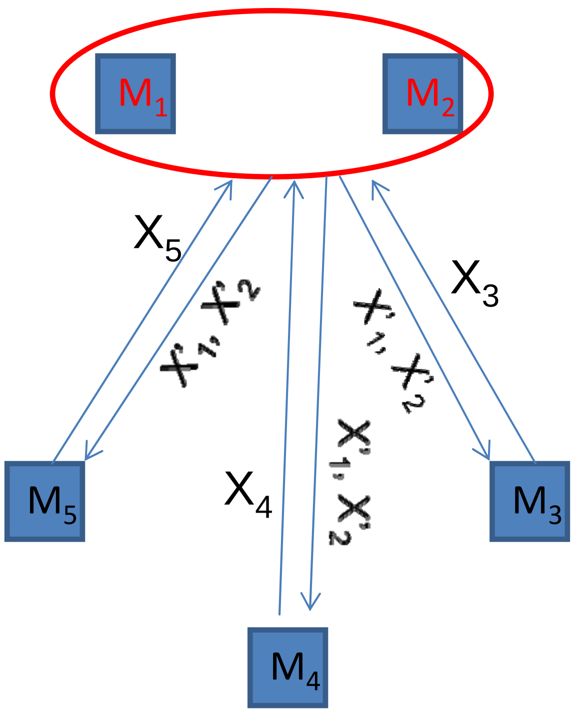
Analysis results for DB

- Single dishonest insider
  - misbehaving in 1st phase -> selective control
  - misbehaving only in 2nd phase -> no key control
- Two adjacent dishonest insiders
  - misbehaving in 2nd phase -> strong control

Attack on DB: Strong key control

M_1 and M_2 are dishonest and all other participants are the intended victims.
Goal: Fix the computed key to be the desired value $K' = g^r$.

In the second phase, M_1 and M_2 broadcast corrupted X'_1 and X'_2, derived from other messages.

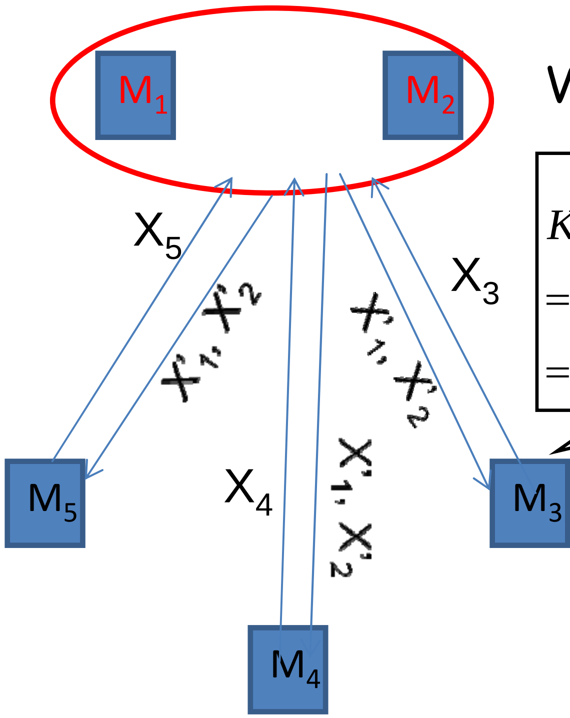


M_1 and M_2 compute:

$$X'_1 = K'/(g^{r_2 r_3 + r_3 r_4 + r_4 r_5 + 2 r_5 r_1})$$
$$X'_2 = g^{r_2 r_3}/(g^{r_1 r_5} X'_1)$$

$$\text{Note that}: X'_1 X'_2 = g^{r_2 r_3 - r_1 r_5} = X_1 X_2$$

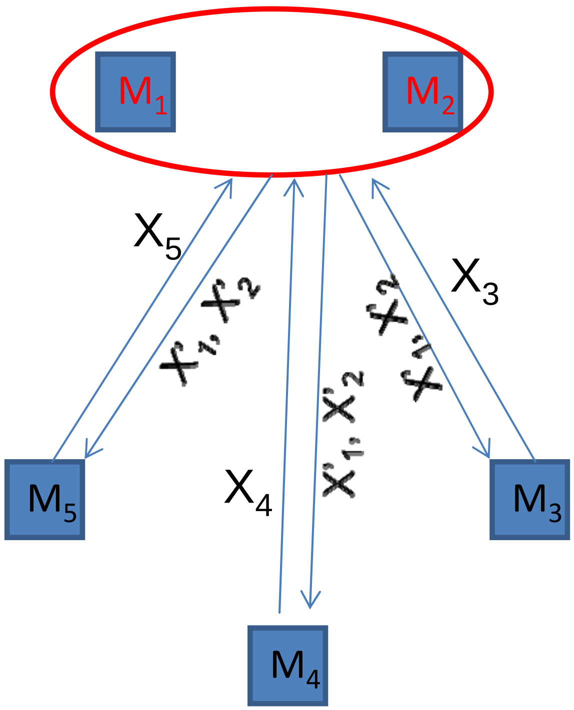
Verification step by honest members



Verification by M_3 succeeds

$$
\begin{aligned}
K_2^R &= K_3^R X_4 X_5 X'_1\, X'_2 \\
&= K_3^R X_4 X_5 X_1 X_2 \\
&= K_2^R = g^{r_2 r_3} = K_3^L
\end{aligned}
$$

Key computation by honest members



- Key computation by M_3

$$
\begin{aligned}
GK_3 &= K_3^R K_4^R K_5^R K_1^R K_2^R \\
&= K_3^R K_4^R K_5^R (K_5^R X'_1) K_2^R \\
&= g^{r_3 r_4 + r_4 r_5 + r_5 r_1 + r_5 r_1 + r_2 r_3} \left(K' / g^{r_2 r_3 + r_3 r_4 + r_4 r_5 + 2 r_5 r_1} \right) = K'
\end{aligned}
$$

Conclusions

- Novel application of DS model
  - Detecting key control attacks
  - Proving security against key control attacks
- Key control attacks against Dutta-Barua protocol

Thank you … Questions

Remarks

- Consider the following equation

$$r_1r_2 + r_2r_3 + 2r_3\mathbf{r_4}$$
$$+ (n_0 + n_1r_1 + n_2r_2 + n_3r_3 + n_4x_1 + n_5x_2 + n_6x_3)\mathbf{r_4}^{\mathbf{p1}}$$
$$+ (l_0 + l_1r_1 + l_2r_2 + l_3r_3 + l_4x_1 + l_5x_2 + l_6x_3)r_4^{s1} = m_0\mathbf{r_4}^{\mathbf{q1}}$$

- To balance $2r_3r_4$ and $m_0r_4^{q1}$, r_4 must be mapped to 1 ($p_1 = 1$)
- $r_1r_2 + r_2r_3$ is independent of r_4 so to cancel it, r_4 must be mapped to 0 ($s_1 = 0$)

- Different mappings for set E_1 require different functions in F_1. For the above case, 2 functions are enough.