Attacking M&M Collective Signature Scheme

Michal Rjaško Martin Stanek

Comenius University in Bratislava
Faculty of Mathematics, Physics and Informatics
Department of Computer Science
{rjasko,stanek}@dcs.fmph.uniba.sk

June 11, 2010

Collective signatures

- Signing a message by multiple signers
  - in a more efficient manner than concatenating individual signatures of the signers
- N.A. Moldovyan, A.A. Moldovyan: *Blind Collective Signature Protocol Based on Discrete Logarithm Problem*, IJNS, Vol. 11, No. 2, 2010.
  - collective signature scheme based on the Schnorr DSS.
  - three variants: collective, blind and simultaneous contract signing
- We present several security weaknesses of the scheme

Collective signatures

- Signing a message by multiple signers
  - in a more efficient manner than concatenating individual signatures of the signers
- N.A. Moldovyan, A.A. Moldovyan: *Blind Collective Signature Protocol Based on Discrete Logarithm Problem*, IJNS, Vol. 11, No. 2, 2010.
  - collective signature scheme based on the Schnorr DSS.
  - three variants: collective, blind and simultaneous contract signing
- We present several security weaknesses of the scheme

Collective signatures

- Signing a message by multiple signers
  - in a more efficient manner than concatenating individual signatures of the signers
- N.A. Moldovyan, A.A. Moldovyan: *Blind Collective Signature Protocol Based on Discrete Logarithm Problem*, IJNS, Vol. 11, No. 2, 2010.
  - collective signature scheme based on the Schnorr DSS.
  - three variants: collective, blind and simultaneous contract signing
- We present several security weaknesses of the scheme

Schnorr signature scheme

- (probably) the simplest DSS secure in the random oracle model
- parameters:
  - G group of prime order q
  - g generator of G
  - $(sk, pk) = (x, y = g^x)$
- signing a message M:
  1. $R = g^t$, where $t \xleftarrow{\$} \mathbb{Z}_q$
  2. $S = t + xE \bmod q$, where $E = H(M \| R)$
  3. $\sigma = \langle E, S \rangle$
- signature verification (M, σ):

$$H(M \| y^{-E} g^S) = H(M \| g^{-xE} g^{t+xE}) = H(M \| g^t) = H(M \| R) \stackrel{?}{=} E$$

Schnorr signature scheme

- (probably) the simplest DSS secure in the random oracle model
- parameters:
  - G group of prime order q
  - g generator of G
  - $(sk, pk) = (x, y = g^x)$
- signing a message M:
  1. $R = g^t$, where $t \xleftarrow{\$} \mathbb{Z}_q$
  2. $S = t + xE \bmod q$, where $E = H(M \| R)$
  3. $\sigma = \langle E, S \rangle$
- signature verification (M, σ):

$$H(M \| y^{-E} g^S) = H(M \| g^{-xE} g^{t+xE}) = H(M \| g^t) = H(M \| R) \stackrel{?}{=} E$$

M&M collective signature scheme

- participants $P_1, \ldots, P_m$: $(sk_i, pk_i) = (x_i, y_i = g^{x_i})$
- signing a message M:
  1. $R = R_1 R_2 \ldots R_m$, where P_i computes $R_i = g^{t_i}$, $t_i \xleftarrow{\$} \mathbb{Z}_q$
  2. $E = H(M \,||\, R)$
  3. $S = S_1 + S_2 + \ldots + S_m \bmod q$,
     where P_i computes $S_i = t_i + x_i E \bmod q$
  4. $\sigma = \langle E, S \rangle$
- signature verification (M, σ):
  1. $y = y_1 y_2 \ldots y_m$ (collective public key)
  2. verification:

$$H(M \,||\, y^{-E} g^{S}) = H(M \,||\, g^{-E \sum_i x_i} g^{\sum_i t_i + E \sum_i x_i})$$
$$= H(M \,||\, g^{\sum_i t_i}) = H(M \,||\, R) \stackrel{?}{=} E$$

M&M collective signature scheme

- participants $P_1, \ldots, P_m$: $(sk_i, pk_i) = (x_i, y_i = g^{x_i})$
- signing a message M:
  1. $R = R_1 R_2 \ldots R_m$, where P_i computes $R_i = g^{t_i}$, $t_i \xleftarrow{\$} \mathbb{Z}_q$
  2. $E = H(M \,||\, R)$
  3. $S = S_1 + S_2 + \ldots + S_m \bmod q$,
     where P_i computes $S_i = t_i + x_i E \bmod q$
  4. $\sigma = \langle E, S \rangle$
- signature verification (M, σ):
  1. $y = y_1 y_2 \ldots y_m$ (collective public key)
  2. verification:

$$\begin{aligned} H(M \,||\, y^{-E} g^S) &= H(M \,||\, g^{-E \sum_i x_i} g^{\sum_i t_i + E \sum_i x_i}) \\ &= H(M \,||\, g^{\sum_i t_i}) = H(M \,||\, R) \stackrel{?}{=} E \end{aligned}$$

Security analysis of M&M scheme

The authors proved:

- Participants $P_1, \ldots, P_{m-1}$ are unable to create a signature of message M for $P_1, \ldots, P_{m-1}, P_m$.
- Malicious participants $P_1, \ldots, P_{m-1}$ of a collective signature (E, S) can not compute the secret key of P_m.

Is this enough?

Security analysis of M&M scheme

The authors proved:

- Participants $P_1, \ldots, P_{m-1}$ are unable to create a signature of message M for $P_1, \ldots, P_{m-1}, P_m$.
- Malicious participants $P_1, \ldots, P_{m-1}$ of a collective signature (E, S) can not compute the secret key of P_m.

Is this enough?

No, it isn't ... Joining Attack

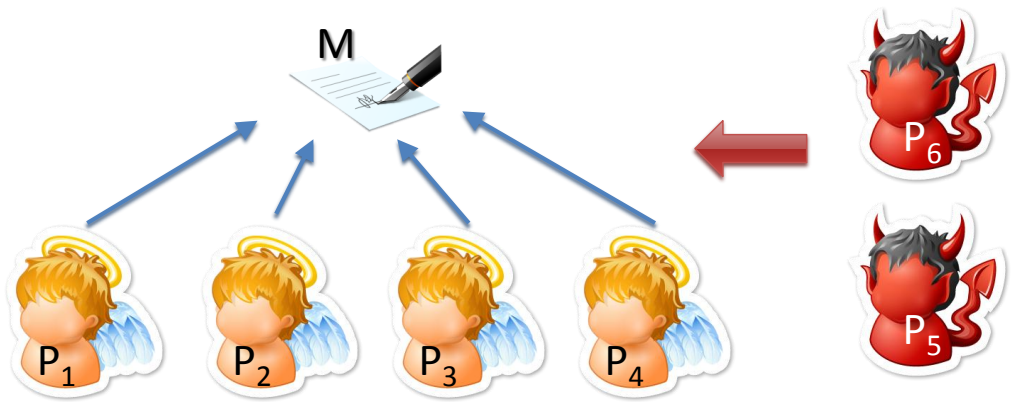
Two or more participants can add themselves to any collective signature (without a consent or participation of the original signers)

- Given a collective signature $\langle E, S \rangle$ of message M; P_{m+1}, P_{m+2} want to join
- P_{m+1} and P_{m+2} choose t_{m+1} and t_{m+2} such that

$$t_{m+2} \equiv -t_{m+1} \pmod{q}$$

- thus R and E stay unchanged:

$$R = g^{t_1} \dots g^{t_m} g^{t_{m+1}} g^{t_{m+2}} = g^{t_1} \dots g^{t_m}$$
$$E = H(M \| R)$$



No, it isn't ... Joining Attack

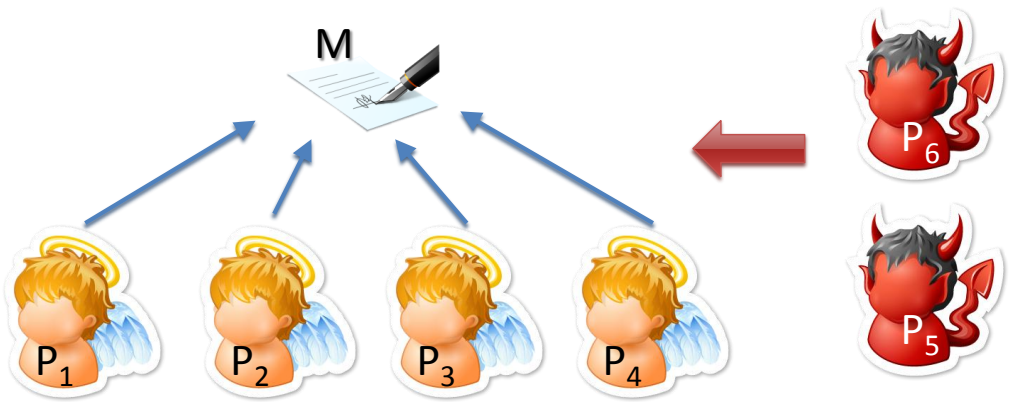
Two or more participants can add themselves to any collective signature (without a consent or participation of the original signers)

- Given a collective signature $\langle E, S \rangle$ of message M; P_{m+1}, P_{m+2} want to join
- P_{m+1} and P_{m+2} choose t_{m+1} and t_{m+2} such that

$$t_{m+2} \equiv -t_{m+1} \pmod{q}$$

- thus R and E stay unchanged:

$$\begin{aligned} R &= g^{t_1} \dots g^{t_m} g^{t_{m+1}} g^{t_{m+2}} = g^{t_1} \dots g^{t_m} \\ E &= H(M \| R) \end{aligned}$$



Joining Attack

- P_{m+1} and P_{m+2} construct new signature:

$$\langle E, S^* \rangle = \langle E, S + t_{m+1} + t_{m+2} + E(x_{m+1} + x_{m+2}) \rangle$$

The verification of $\langle E^*, S^* \rangle$ will be successful

$$\begin{aligned} H(M \,||\, Y^{*-E^*} g^{S^*}) &= H\left(M \,||\, Y^{-E} Y_{m+1}^{-E} Y_{m+2}^{-E} \cdot g^{S+t_{m+1}+t_{m+2}+E(x_{m+1}+x_{m+2})}\right) \\ &= H\left(M \,||\, Y^{-E} \cdot g^{S+t_{m+1}+t_{m+2}}\right) \\ &= H\left(M \,||\, Y^{-E} \cdot g^{S}\right) \\ &= H(M \,||\, R) = E = E^* \end{aligned}$$

Joining Attack

- Attack can be easily extended to more than two participants
- Potentially unwanted property
  - When signing a petition it can be desirable
  - In some other cases not
- Fix: add number of signers to E
  - $E = H(M \| R \| m)$ or
  - $E = H(M \| R \| Y_1 \| \ldots \| Y_m)$.

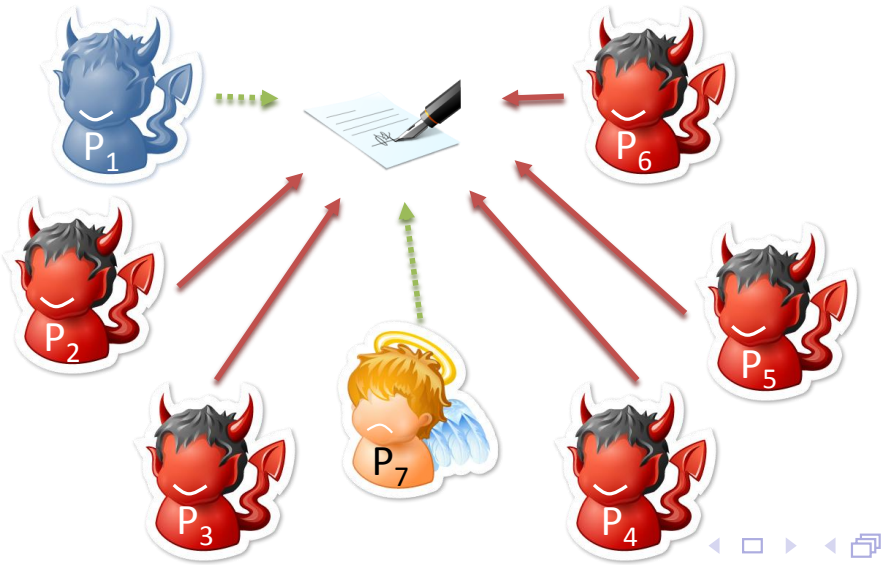
Joining Attack

- Attack can be easily extended to more than two participants
- Potentially unwanted property
  - When signing a petition it can be desirable
  - In some other cases not
- Fix: add number of signers to E
  - $E = H(M \,||\, R \,||\, m)$ or
  - $E = H(M \,||\, R \,||\, Y_1 \,||\, \ldots \,||\, Y_m)$.

Related Public Key Attack

Group of malicious participants $P_1, \ldots, P_{m-1}$ can create a collective signature of any message M for $P_1, \ldots, P_m$.

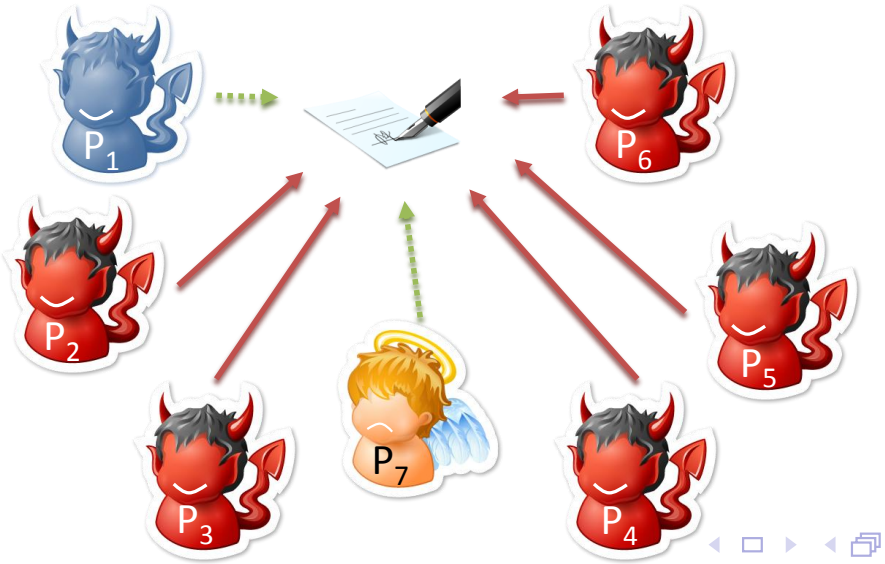
1. P_1 sets/registers his public key to $Y_1 = Y_m^{-1} \bmod p$
   - Thus, $x_1 \equiv -x_m \pmod{q}$ (even though P_1 does not know x_1)
2. $P_2, \ldots, P_{m-1}$ construct collective signature of M: $\langle E, S \rangle$
3. The final collective signature of M for $P_1, \ldots, P_m$ is $\langle E, S \rangle$



Related Public Key Attack

Group of malicious participants $P_1, \ldots, P_{m-1}$ can create a collective signature of any message M for $P_1, \ldots, P_m$.

1. P_1 sets/registers his public key to $Y_1 = Y_m^{-1} \bmod p$
   - Thus, $x_1 \equiv -x_m \pmod{q}$ (even though P_1 does not know x_1)
2. $P_2, \ldots, P_{m-1}$ construct collective signature of M: $\langle E, S \rangle$
3. The final collective signature of M for $P_1, \ldots, P_m$ is $\langle E, S \rangle$



Related Public Key Attack

The verification of $\langle E, S \rangle$ for $P_1, \ldots, P_m$ will be successful

$$\begin{aligned} H(M \,||\, Y^{-E} g^S) &= H(M \,||\, \tilde{Y}^{-E} \cdot (Y_1 Y_m)^{-E} \cdot g^S) \\ &= H(M \,||\, \tilde{Y}^{-E} \cdot g^S) \\ &= H(M \,||\, R) = E \end{aligned}$$

where

$$\begin{aligned} Y &= Y_1 \cdot \ldots \cdot Y_m \bmod p \\ \tilde{Y} &= Y_2 \cdot \ldots \cdot Y_{m-1} \end{aligned}$$

Moreover, $P_1, \ldots, P_{m-1}$ can hide the suspicious public key Y_1.

- Choose a random nonempty subset $\mathcal{A} \subset \{P_1, \ldots, P_{m-1}\}$.
- The attackers from $\mathcal{A}$ select their public keys so that $\prod_{i \in \mathcal{A}} Y_i \equiv Y_m^{-1} \pmod{p}$.
  - this can be done such that exactly one attacker from $\mathcal{A}$ does not know his secret key
- The attack proceeds as before – signature of M created by $\{P_1, \ldots, P_{m-1}\} \setminus \mathcal{A}$ is again a valid signature of M for $P_1, \ldots, P_m$.

Related Public Key Attack

- Definitely unwanted property
- Previous fix does not work here; Malicious participants can compute E.
- Fix: sum secret keys into S in non-uniform way
  - i.e. $S_i = t_i + E w_i x_i \bmod q$, where $w_i = H(Y_i \,||\, E)$.
  - Certainly, the security properties of this modification must be analyzed in detail.

Related Public Key Attack

- Definitely unwanted property
- Previous fix does not work here; Malicious participants can compute E.
- Fix: sum secret keys into S in non-uniform way
  - i.e. $S_i = t_i + E w_i x_i \bmod q$, where $w_i = H(Y_i \,||\, E)$.
  - Certainly, the security properties of this modification must be analyzed in detail.

Related Public Key Attack

- Definitely unwanted property
- Previous fix does not work here; Malicious participants can compute E.
- Fix: sum secret keys into S in non-uniform way
  - i.e. $S_i = t_i + E w_i x_i \bmod q$, where $w_i = H(Y_i \| E)$.
  - Certainly, the security properties of this modification must be analyzed in detail.

Conclusion

- We presented two attacks on the M&M collective signature scheme
  - Joining attack
  - Related public key attack
- These attacks can be also applied to the other variants of M&M scheme (blind and simultaneous contract signing)
- Another example how important is proper security analysis.

Thank you for your attention