Security Protocols

Lecture 6 - Fixing Dolev-Yao

Matteo Acclavio

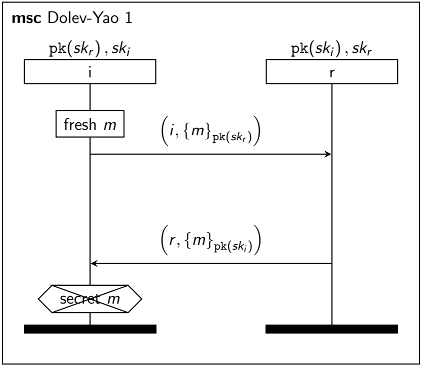
October 6^{th}, 2021

Fixing Dolev-Yao Protocol

The purpose of this lecture is to "fix" Dolev-Yao protocol in order to assure the secrecy of the exchanged message m

- We look back at the attack on the Dolev-Yao protocol we discuss last Monday (DY1)
- We define a new version of this protocol (DY2) adding an additional encryption level to the messages
- We show that additional encryption does not fix the protocol
- We define a third version of the protocol (DY3) with a wiser use of the encryption
- We prove that there are no possible attacks to this protocol

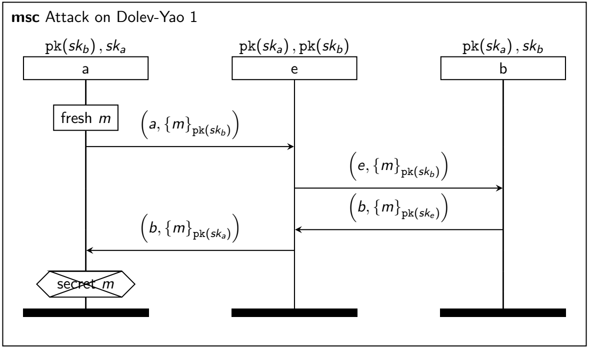
Attacking DY1



$I_{DY1}(c, i, sk_i, r, pk_r) :=$ fresh m;
$\text{out}\Big(c, \Big(i, \{m\}_{pk_r}\Big)\Big)$;
$\text{in}(c, x)$;
if $\texttt{fst}(x) = r$ then
if $\texttt{dec}(\texttt{snd}(x), sk_i) = m$ then
$\text{secret}(m)$

$R_{DY1}(c, r, sk_r, i, pk_i) :=$ $\text{in}(c, x)$;
if $\texttt{fst}(x) = i$ then
$\texttt{let}\ m = \texttt{dec}(\texttt{snd}(x), sk_r)\ \texttt{in}$
$\text{out}\Big(c, \Big(r, \{m\}_{pk_i}\Big)\Big)$;

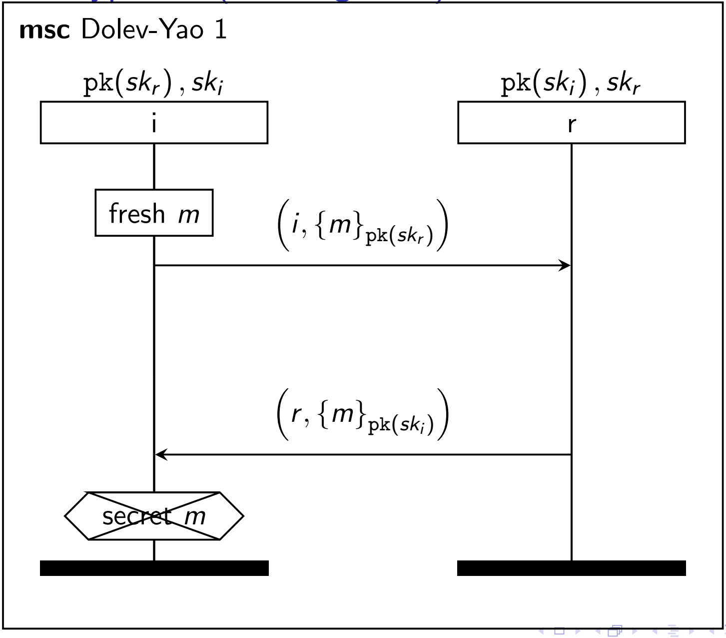
Attacking DY1



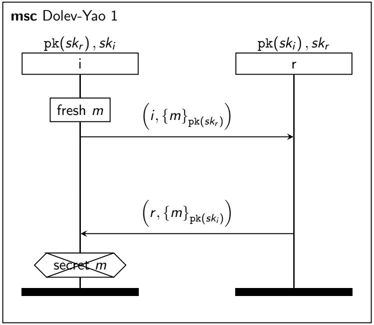
$$\text{fresh } sk_a, sk_b;\ \left[\ \left\{\begin{array}{l} pk_a \mapsto \mathtt{pk}(sk_a)\,, \\ pk_b \mapsto \mathtt{pk}(sk_b) \end{array}\right\},\ \begin{array}{l} !\mathit{Initiator}(c, a, sk_a, b, \mathtt{pk}(sk_b)) \mid \\ !\mathit{Initiator}(c, b, sk_b, a, \mathtt{pk}(sk_a)) \mid \\ !\mathrm{in}(c, e); \\ \ \mathrm{in}(c, pk_e); \\ \ \mathit{Responder}(c, a, sk_a, e, pk_e) \mid \\ !\mathrm{in}(c, e); \\ \ \mathrm{in}(c, pk_e); \\ \ \mathit{Responder}(c, b, sk_b, e, pk_e) \end{array}\ \right] \vDash \begin{array}{l} \langle \mathsf{out}(c, u_1)\, \rangle \\ \langle \mathsf{in}(c, e)\, \rangle \\ \langle \mathsf{in}(c, \mathtt{pk}(sk_e))\, \rangle \\ \langle \mathsf{in}(c, (e, \mathtt{snd}(u_1)))\, \rangle \\ \langle \mathsf{out}(c, u_2)\, \rangle \\ \left\langle \mathsf{in}\left(c, T\left(b, \{\mathtt{dec}(\mathtt{snd}(u_2)\,, sk_e)\}_{pk_a}\right)\right) \right\rangle \\ \langle \mathrm{secret}(\mathtt{dec}(\mathtt{snd}(u_2)\,, sk_e))\, \rangle \mathtt{true} \end{array}$$

Attacking DY1

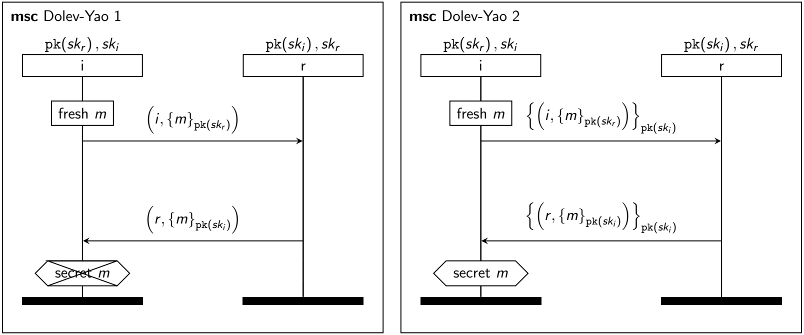
More encryption! (defining DY2)



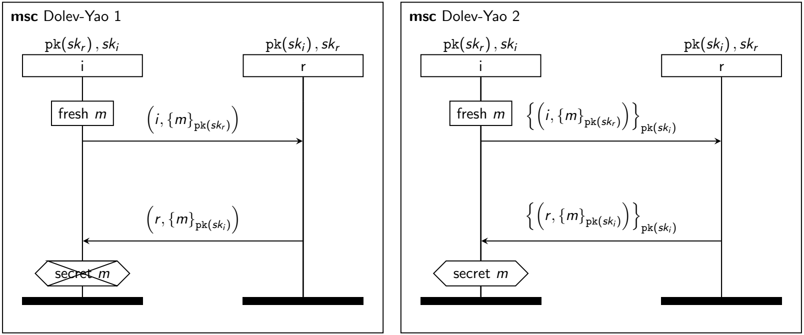
More encryption! (defining DY2)



More encryption! (defining DY2)

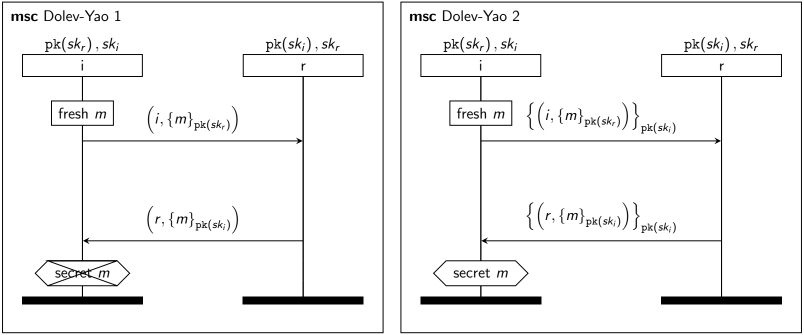


More encryption! (defining DY2)



How did we improve the protocol?

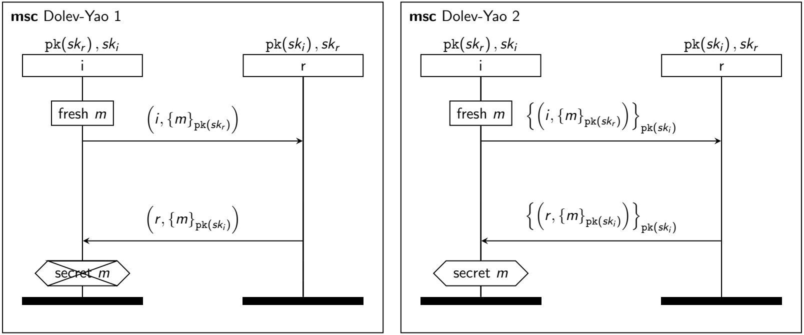
More encryption! (defining DY2)



How did we improve the protocol?

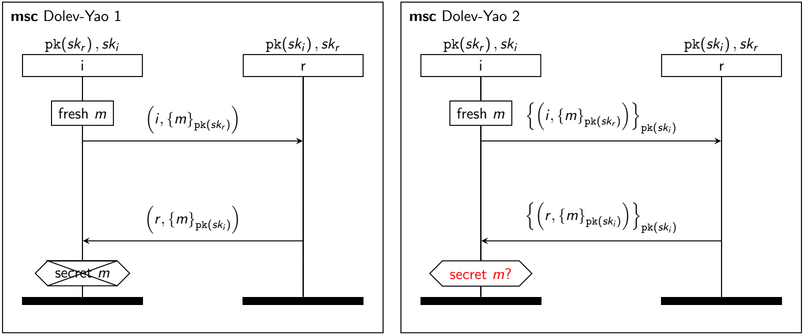
The attacker can no more intercept the initiator message and fake itself as the initiator

More encryption! (defining DY2)



How did we improve the protocol?
The attacker can no more intercept the initiator message and fake itself as the initiator
WE FIXED IT!

More encryption! (defining DY2)



How did we improve the protocol?

The attacker can no more intercept the initiator message and fake itself as the initiator

DID WE FIX IT?

Looking for an attack to DY2

In the attack to DY1 we use the honest behaviour of the responder b to decrypt the message: by changing the sender identifier in the message $\left(a, \{m\}_{\mathtt{pk}(sk_b)}\right)$ with its own using the fact that

$$b \text{ receives } \left(x, \{y\}_{\mathtt{pk}(sk_b)}\right) \Rightarrow b \text{ replies } \left(b, \{y\}_{\mathtt{pk}(sk_x)}\right)$$

Looking for an attack to DY2

In the attack to DY1 we use the honest behaviour of the responder b to decrypt the message: by changing the sender identifier in the message $\left(a, \{m\}_{\mathtt{pk}(sk_b)}\right)$ with its own using the fact that

$$b \text{ receives } \left(x, \{y\}_{\mathtt{pk}(sk_b)}\right) \Rightarrow b \text{ replies } \left(b, \{y\}_{\mathtt{pk}(sk_x)}\right)$$

b does not care who x is!

Looking for an attack to DY2

In the attack to DY1 we use the honest behaviour of the responder b to decrypt the message: by changing the sender identifier in the message $\left(a, \{m\}_{\mathtt{pk}(sk_b)}\right)$ with its own using the fact that

$$b \text{ receives } \left(x, \{y\}_{\mathtt{pk}(sk_b)}\right) \Rightarrow b \text{ replies } \left(b, \{y\}_{\mathtt{pk}(sk_x)}\right)$$

b does not care who x is!

If x is the attacker, the attacker can now read y.

Looking for an attack to DY2

In the attack to DY1 we use the honest behaviour of the responder b to decrypt the message: by changing the sender identifier in the message $\left(a, \{m\}_{\mathtt{pk}(sk_b)}\right)$ with its own using the fact that

$$b \text{ receives } \left(x, \{y\}_{\mathtt{pk}(sk_b)}\right) \Rightarrow b \text{ replies } \left(b, \{y\}_{\mathtt{pk}(sk_x)}\right)$$

b does not care who x is!

If x is the attacker, the attacker can now read y.

Can we do a similar trick in DY2?

Discovering an attack to DY2

$$b \text{ receives } \left\{\left(x, \{y\}_{\mathtt{pk}(sk_b)}\right)\right\}_{\mathtt{pk}(sk_b)} \Rightarrow b \text{ replies } \left\{\left(b, \{y\}_{\mathtt{pk}(sk_x)}\right)\right\}_{\mathtt{pk}(sk_x)}$$

Discovering an attack to DY2

$$b \text{ receives } \left\{\left(x, \{y\}_{\mathtt{pk}(sk_b)}\right)\right\}_{\mathtt{pk}(sk_b)} \Rightarrow b \text{ replies } \left\{\left(b, \{y\}_{\mathtt{pk}(sk_x)}\right)\right\}_{\mathtt{pk}(sk_x)}$$

if x is the attacker identifier, then it can now read b AND y (because b removes 2 layers of encryption)

Discovering an attack to DY2

$$b \text{ receives } \left\{\left(x, \{y\}_{\mathtt{pk}(sk_b)}\right)\right\}_{\mathtt{pk}(sk_b)} \Rightarrow b \text{ replies } \left\{\left(b, \{y\}_{\mathtt{pk}(sk_x)}\right)\right\}_{\mathtt{pk}(sk_x)}$$

if x is the attacker identifier, then it can now read b AND y (because b removes 2 layers of encryption)

Can we trick b to remove just 1 layer of encryption?

Discovering an attack to DY2

$$b \text{ receives } \left\{\left(x, \{y\}_{\mathrm{pk}(sk_b)}\right)\right\}_{\mathrm{pk}(sk_b)} \Rightarrow b \text{ replies } \left\{\left(b, \{y\}_{\mathrm{pk}(sk_x)}\right)\right\}_{\mathrm{pk}(sk_x)}$$

if x is the attacker identifier, then it can now read b AND y (because b removes 2 layers of encryption)

Can we trick b to remove just 1 layer of encryption?

message we eavesdrop	message we send to b	message we receive from b
$\left\{\left(a, \{m\}_{\mathrm{pk}(sk_b)}\right)\right\}_{\mathrm{pk}(sk_b)}$	$\left\{\left(e, \left\{\left(a, \{m\}_{\mathrm{pk}(sk_b)}\right)\right\}_{\mathrm{pk}(sk_b)}\right)\right\}_{\mathrm{pk}(sk_b)}$	$\left\{\left(b, \left\{\left(a, \{m\}_{\mathrm{pk}(sk_b)}\right)\right\}_{\mathrm{pk}(sk_e)}\right)\right\}_{\mathrm{pk}(sk_e)}$ from which e can deduce $\{m\}_{\mathrm{pk}(sk_b)}$

Discovering an attack to DY2

$$b \text{ receives } \left\{\left(x, \{y\}_{\mathtt{pk}(sk_b)}\right)\right\}_{\mathtt{pk}(sk_b)} \Rightarrow b \text{ replies } \left\{\left(b, \{y\}_{\mathtt{pk}(sk_x)}\right)\right\}_{\mathtt{pk}(sk_x)}$$

if x is the attacker identifier, then it can now read b AND y (because b removes 2 layers of encryption)

Can we trick b to remove just 1 layer of encryption?

message we eavesdrop	message we send to b	message we receive from b
$\left\{\left(a, \{m\}_{\mathtt{pk}(sk_b)}\right)\right\}_{\mathtt{pk}(sk_b)}$	$\left\{\left(e, \left\{\left(a, \{m\}_{\mathtt{pk}(sk_b)}\right)\right\}_{\mathtt{pk}(sk_b)}\right)\right\}_{\mathtt{pk}(sk_b)}$	$\left\{\left(b, \left\{\left(a, \{m\}_{\mathtt{pk}(sk_b)}\right)\right\}_{\mathtt{pk}(sk_e)}\right)\right\}_{\mathtt{pk}(sk_e)}$ from which e can deduce $\{m\}_{\mathtt{pk}(sk_b)}$

now we know	message we send to b	message receive from b
$\{m\}_{\mathtt{pk}(sk_b)}$	$\left\{\left(e, \{m\}_{\mathtt{pk}(sk_b)}\right)\right\}_{\mathtt{pk}(sk_b)}$	$\left\{\left(b, \{m\}_{\mathtt{pk}(sk_e)}\right)\right\}_{\mathtt{pk}(sk_e)}$ from which e can deduce m

Attacking DY2

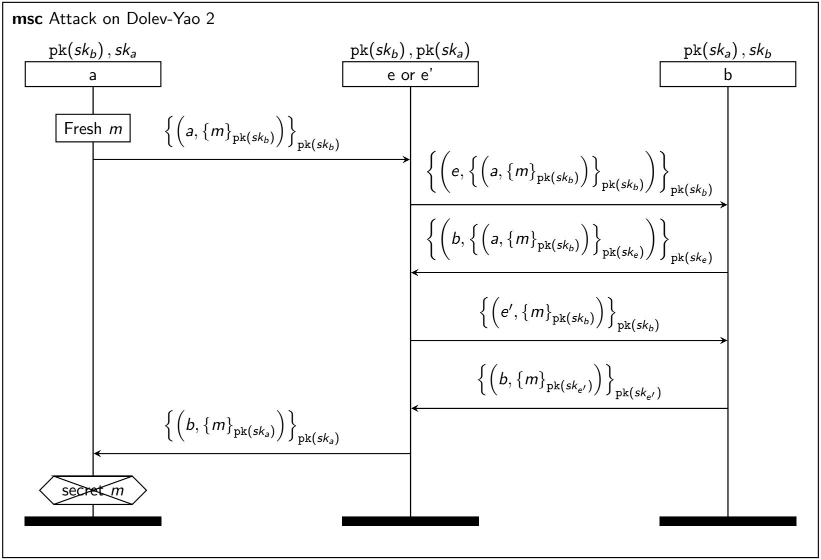
$$\left[\{\emptyset\},\ \begin{array}{l}\mathsf{fresh}\ sk_a, sk_b;\\ \mathrm{out}(\mathit{keys}, \mathtt{pk}(sk_a));\mathrm{out}(\mathit{keys}, \mathtt{pk}(sk_b));\ \mid\\ !I_{DY2}(c, a, sk_a, b, \mathtt{pk}(sk_b))\ \mid\\ !\mathrm{in}(c, e);\mathrm{in}(c, pk_e);R_{DY2}(c, b, sk_b, e, pk_e)\end{array}\right] \longrightarrow^*$$

$$\mathsf{State}_{\mathsf{DY2'}} = \mathsf{fresh}\ sk_a, sk_b, m; \left[\left\{\begin{array}{l} pk_a \mapsto \mathtt{pk}(sk_a),\\ pk_a \mapsto \mathtt{pk}(sk_b),\\ u_1 \mapsto \left\{\left(a, \{m\}_{\mathtt{pk}(sk_b)}\right)\right\}_{\mathtt{pk}(sk_b)},\\ u_2 \mapsto \left\{\left(b, \{\mathtt{dec}(y_1, sk_b)\}_{pk_e}\right)\right\}_{pk_e},\\ u_3 \mapsto \left\{\left(b, \{\mathtt{dec}(y_2, sk_b)\}_{pk_{e'}}\right)\right\}_{pk_{e'}} \end{array}\right\},\ \begin{array}{l} \text{if}\ \mathtt{fst}(\mathtt{dec}(w, sk_a)) = b\ \text{then}\\ \text{if}\ \mathtt{dec}(\mathtt{snd}(\mathtt{dec}(w, sk_a)), sk_a) = m\ \text{then}\\ \mathrm{secret}(m)\ \mid\\ !I_{DY2}(c, a, sk_a, b, \mathtt{pk}(sk_b))\ \mid\\ 0 \mid 0 \mid\\ !\mathrm{in}(c, e);\mathrm{in}(c, pk_e);\\ \ R_{DY2}(c, b, sk_b, e, pk_e) \end{array}\right]$$

and

$$\mathsf{State}_{\mathsf{DY2'}} \models \begin{array}{l} \langle \mathsf{out}(c, u_1) \rangle \langle \mathsf{in}(c, e) \rangle \langle \mathsf{in}(c, \mathtt{pk}(sk_e)) \rangle\\ \left\langle \mathsf{in}\left(c, \{(e, u_1)\}_{pk_b}\right) \right\rangle \langle \mathsf{out}(c, u_2) \rangle \langle \mathsf{in}(c, e') \rangle \langle \mathsf{in}(c, \mathtt{pk}(sk_{e'})) \rangle\\ \left\langle \mathsf{in}\left(c, \{(e', \mathtt{snd}(\mathtt{dec}(\mathtt{snd}(\mathtt{dec}(u_2, sk_e)), sk_e)))\}_{pk_b}\right) \right\rangle\\ \langle \mathsf{out}(c, u_3) \rangle\\ \left\langle \mathsf{in}\left(c, \left\{\left(b, \{\mathtt{dec}(\mathtt{snd}(\mathtt{dec}(u_3, sk_{e'})), sk_{e'})\}_{pk_a}\right)\right\}_{pk_a}\right) \right\rangle\\ \langle \mathrm{secret}(\mathtt{dec}(\mathtt{snd}(\mathtt{dec}(u_3, sk_{e'})), sk_{e'})) \rangle\\ \mathtt{true} \end{array}$$

Attacking DY2



When the secret m is exposed?

The secret is exposed when we have a transition of the shape

$$\frac{m\theta =_{\mathsf{E}} M}{[\theta,\ \mathrm{secret}(M)] \xrightarrow{\mathrm{secret}(m)} [\theta,\ 0]}\ (\textsc{Secret})$$

$$\theta_1 = \left\{ \begin{array}{c} pk_a \mapsto \mathtt{pk}(sk_a), \\ pk_a \mapsto \mathtt{pk}(sk_b), \\ u_1 \mapsto \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)}, \\ \\ \end{array} \right\}$$

When the secret m is exposed?

The secret is exposed when we have a transition of the shape

$$\frac{m\theta =_{\mathsf{E}} M}{[\theta,\ \mathrm{secret}(M)] \xrightarrow{\mathrm{secret}(m)} [\theta,\ 0]}\ (\textsc{Secret})$$

$$\theta_2 = \left\{ \begin{array}{c} pk_a \mapsto \mathtt{pk}(sk_a), \\ pk_a \mapsto \mathtt{pk}(sk_b), \\ u_1 \mapsto \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)}, \\ u_2 \mapsto \left\{ \left(b, \{\mathtt{dec}(y_1, sk_b)\}_{pk_e} \right) \right\}_{pk_e}, \\ \end{array} \right\}$$

When the secret m is exposed?

The secret is exposed when we have a transition of the shape

$$\frac{m\theta =_{\mathsf{E}} M}{[\theta,\ \mathrm{secret}(M)] \xrightarrow{\mathrm{secret}(m)} [\theta,\ 0]}\ (\textsc{Secret})$$

$$\theta_3 = \left\{ \begin{array}{c} pk_a \mapsto \mathtt{pk}(sk_a), \\ pk_a \mapsto \mathtt{pk}(sk_b), \\ u_1 \mapsto \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)}, \\ u_2 \mapsto \left\{ \left(b, \{\mathtt{dec}(y_1, sk_b)\}_{pk_e} \right) \right\}_{pk_e}, \\ u_3 \mapsto \left\{ \left(b, \{\mathtt{dec}(y_2, sk_b)\}_{pk_{e'}} \right) \right\}_{pk_{e'}} \end{array} \right\}$$

When the secret m is exposed?

The secret is exposed when we can derive $\Gamma \vdash m$.

$$\Gamma_1 = \text{fresh}\, sk_a, sk_b, m; \mathtt{pk}(sk_a)\,, \mathtt{pk}(sk_b)\,, \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)}$$

$$\Gamma_2 = \Gamma_1, \left\{ \left(b, \{\mathtt{dec}(y_1, sk_b)\}_{pk_e} \right) \right\}_{pk_e}$$

$$\Gamma_3 = \Gamma_2, \left\{ \left(b, \{\mathtt{dec}(y_2, sk_b)\}_{pk_{e'}} \right) \right\}_{pk_{e'}}$$

When the secret m is exposed?

The secret is exposed when we can derive $\Gamma \vdash m$.

$$\Gamma_1 = \text{fresh } sk_a, sk_b, m; \mathtt{pk}(sk_a), \mathtt{pk}(sk_b), \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)}$$

$$\Gamma_2 = \Gamma_1, \left\{ \left(b, \{\mathtt{dec}(y_1, sk_b)\}_{pk_e} \right) \right\}_{pk_e}$$

$$\Gamma_3 = \Gamma_2, \left\{ \left(b, \{\mathtt{dec}(y_2, sk_b)\}_{pk_{e'}} \right) \right\}_{pk_{e'}}$$

$$\frac{}{\text{fresh } \vec{x}; \Gamma, M \vdash M}\ (\text{Ax}) \qquad \frac{z \text{ fresh for } \vec{x}}{\text{fresh } \vec{x}; \Gamma \vdash z}\ (\text{Sol})$$

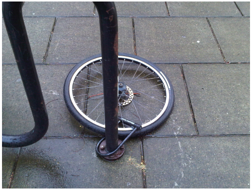
$$\frac{\text{fresh } \vec{x}; \Gamma \vdash M \quad \text{fresh } \vec{x}; \Gamma \vdash N}{\text{fresh } \vec{x}; \Gamma \vdash (M, N)}\ (\text{I-pair}) \qquad \frac{\text{fresh } \vec{x}; \Gamma \vdash M \quad \text{fresh } \vec{x}; \Gamma \vdash K}{\text{fresh } \vec{x}; \Gamma \vdash \{M\}_K}\ (\text{I-enc}) \qquad \frac{\text{fresh } \vec{x}; \Gamma \vdash K}{\text{fresh } \vec{x}; \Gamma \vdash \mathtt{pk}(K)}\ (\text{I-pk})$$

$$\frac{\text{fresh } \vec{x}; \Gamma, M, N \vdash K}{\text{fresh } \vec{x}; \Gamma, (M, N) \vdash K}\ (\text{E-pair}) \qquad \frac{\text{fresh } \vec{x}; \Gamma, M \vdash L \quad \text{fresh } \vec{x}; \Gamma \vdash K}{\text{fresh } \vec{x}; \Gamma, \{M\}_{\mathtt{pk}(K)} \vdash L}\ (\text{E-enc})$$

$$\frac{\text{fresh } \vec{x}; \Gamma, M \vdash L}{\text{fresh } \vec{x}; \Gamma, \mathtt{dec}\left(\{M\}_{\mathtt{pk}(K)}, K\right) \vdash L}\ (\text{E-dec}) \qquad \frac{\text{fresh } \vec{x}; \Gamma \vdash M \quad \text{fresh } \vec{x}; \Gamma \vdash K}{\text{fresh } \vec{x}; \Gamma \vdash \mathtt{dec}(M, K)}\ (\text{I-dec})$$

Understand our errors in fixing Dolev-Yao

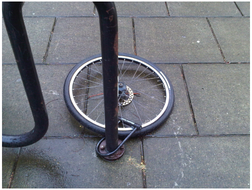
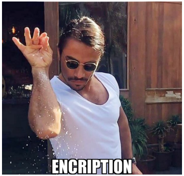
We add encryption without reflecting



+

Understand our errors in fixing Dolev-Yao

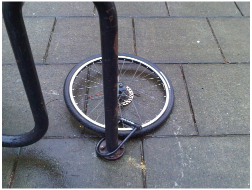
We add encryption without reflecting

 + 

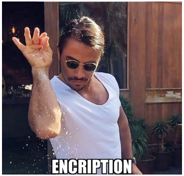
=

Understand our errors in fixing Dolev-Yao

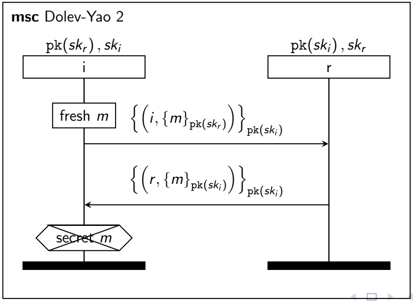
We add encryption without reflecting



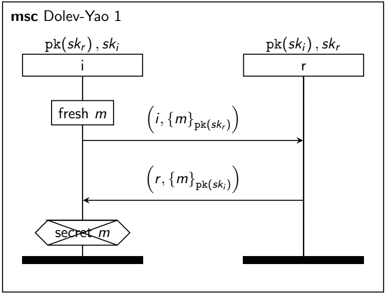
$+$

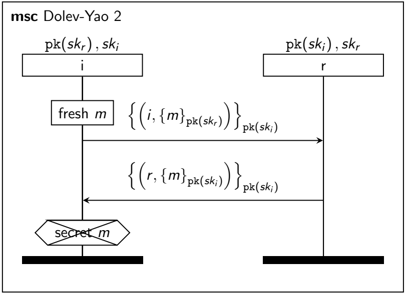


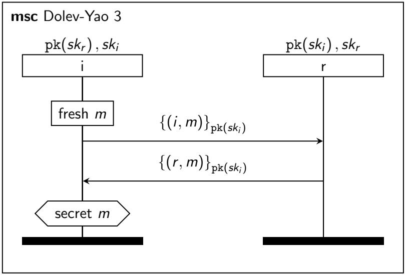
$=$



A wiser use of encryption (defining DY2)







How did we improve the protocol?
DID WE FIXED IT?

What does it means to prove secrecy?

- Prove that a secret can be revealed = show EXISTS attack

There is ONE formula $\phi = \langle \pi_1 \rangle \ldots \langle \pi_n \rangle \langle \mathrm{secret}(m) \rangle \psi$
and there is ONE extended protocols $[\theta,\ P]$
such that DY3 $\longrightarrow^*$ $[\theta,\ P]$ and such that

$$[\theta,\ P] \models \phi$$

What does it means to prove secrecy?

- Prove that a secret can be revealed = show EXISTS attack

  There is ONE formula $\phi = \langle \pi_1 \rangle \ldots \langle \pi_n \rangle \langle \mathrm{secret}(m) \rangle \psi$
  and there is ONE extended protocols $[\theta,\ P]$
  such that DY3 $\longrightarrow^* [\theta,\ P]$ and such that

  $$[\theta,\ P] \models \phi$$

- Prove that a secret cannot be revealed = show that EACH possible attack fails

  For ALL formulas $\phi = \langle \pi_1 \rangle \ldots \langle \pi_n \rangle \langle \mathrm{secret}(m) \rangle \psi$
  and for ALL extended protocols $[\theta,\ P]$
  such that DY3 $\longrightarrow^* [\theta,\ P]$ we have

  $$[\theta,\ P] \not\models \phi$$

Infinite is a drag I: induction is tricky

Theorem

There are infinitely many prime numbers.

Proof.

If finite they are $p_1, \ldots, p_n$.
Than take $m = p_1 \cdots p_n + 1$.
Since none of p_i divides m, then m is prime.
Since $m > p_i$ for all i, then m is a new prime.
Absurd □

Infinite is a drag I: induction is tricky

Theorem

For any natural number n the number $m = 2^{(2^n)} + 1$ is prime

Proof.

Fermat:

- $n = 0, \; m = 3$
- $n = 1, \; m = 5$
- $n = 2, \; m = 17$
- $n = 3, \; m = 257$
- $n = 4, \; m = 65537$
- $\dots$

□

Infinite is a drag I: induction is tricky

Theorem (Stated in 1637, proved in 1995)

There are no positive integers x, y, z satisfying the equation

$$x^n + y^n = z^n$$

for $n > 2$.

Proof.

Fermat: I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.
Andrew Wiles: slow down, it's not so easy. □

Infinite is a drag I: induction is tricky

Theorem (Stated in 1637, proved in 1995)

For ALL positive integers x, y, z and for ALL integers $n > 2$ the following equation cannot be satisfied

$$x^n + y^n = z^n$$

Proof.

Fermat: I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.
Andrew Wiles: slow down, it's not so easy. □

Infinite is a drag II: induction VS coinduction

Induction = build "big objects" by composing smaller ones.
A list L is either $\emptyset$ or $L = L', x$ for a list L.

Coinduction = decompose "big objects" to smaller ones.
A stream $S = x_0, x_1, \ldots$ is an object such that $x_1, \ldots$ is a stream.

We here expect to need to take into account a (potential) infinite knowledge as basis of our reasoning.

All the infinite(s) to check in DY3

If the attacker knowledge is Γ, then it knows Y only if $\Gamma \vdash Y$ is derivable.

The potential knowledge of the attacker is given by:

- all possible messages sent by a;
- all possible messages sent by b responding to a;
- all possible messages sent by b responding the attacker faking to be a;
- all possible messages sent b to the attacker making use of its knowledge;

$$\Gamma = \text{fresh}\, sk_a, sk_b, m_1, \ldots, m_n; \quad \begin{array}{l} \{(a, m_i)\}_{\mathtt{pk}(sk_b)}, \\ \{(b, m_i)\}_{\mathtt{pk}(sk_a)}, \\ \{(b, X_i)\}_{\mathtt{pk}(sk_a)}, \\ \{(b, X_j)\}_{\mathtt{pk}(sk_e)} \end{array}$$

Encryption as measure of secrecy

We define the *encryption level of m in N*, as the minimum number of encryption levels the attacker cannot bypass in which the message m is nested in N (∞ if m does not occurs in N).

$$\left\| \{(a, m)\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = \qquad \left\| \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\left\| \left(\{(a, m)\}_{\mathtt{pk}(sk_b)}, \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right) \right\|_{m\text{-enc}} =$$

$$\left\| \{(r, \mathtt{snd}((y, m)))\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\left\| \left\{ \left(r, \mathtt{snd}\left(\mathtt{dec}\left(\{(y, m)\}_{\mathtt{pk}(sk_b)}, sk_b \right) \right) \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\|(a, b)\|_{m\text{-enc}} =$$

Encryption as measure of secrecy

We define the *encryption level of m in N*, as the minimum number of encryption levels the attacker cannot bypass in which the message m is nested in N (∞ if m does not occurs in N).

$$\left\| \{(a, m)\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 1 \qquad \left\| \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\left\| \left(\{(a, m)\}_{\mathtt{pk}(sk_b)}, \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right) \right\|_{m\text{-enc}} =$$

$$\left\| \{(r, \mathtt{snd}((y, m)))\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\left\| \left\{ \left(r, \mathtt{snd}\left(\mathtt{dec}\left(\{(y, m)\}_{\mathtt{pk}(sk_b)}, sk_b \right) \right) \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\|(a, b)\|_{m\text{-enc}} =$$

Encryption as measure of secrecy

We define the *encryption level of m in N*, as the minimum number of encryption levels the attacker cannot bypass in which the message m is nested in N (∞ if m does not occurs in N).

$$\left\| \{(a, m)\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 1 \qquad \left\| \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 2$$

$$\left\| \left(\{(a, m)\}_{\mathtt{pk}(sk_b)} , \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right) \right\|_{m\text{-enc}} =$$

$$\left\| \{(r, \mathtt{snd}((y, m)))\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\left\| \left\{ \left(r, \mathtt{snd}\left(\mathtt{dec}\left(\{(y, m)\}_{\mathtt{pk}(sk_b)} , sk_b \right) \right) \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\|(a, b)\|_{m\text{-enc}} =$$

Encryption as measure of secrecy

We define the *encryption level of m in N*, as the minimum number of encryption levels the attacker cannot bypass in which the message m is nested in N (∞ if m does not occurs in N).

$$\left\| \{(a, m)\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 1 \qquad \left\| \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 2$$

$$\left\| \left(\{(a, m)\}_{\mathtt{pk}(sk_b)} , \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right) \right\|_{m\text{-enc}} = 1$$

$$\left\| \{(r, \mathtt{snd}((y, m)))\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\left\| \left\{ \left(r, \mathtt{snd}\left(\mathtt{dec}\left(\{(y, m)\}_{\mathtt{pk}(sk_b)} , sk_b \right) \right) \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\|(a, b)\|_{m\text{-enc}} =$$

Encryption as measure of secrecy

We define the *encryption level of m in N*, as the minimum number of encryption levels the attacker cannot bypass in which the message m is nested in N (∞ if m does not occurs in N).

$$\left\| \{(a, m)\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 1 \qquad \left\| \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 2$$

$$\left\| \left(\{(a, m)\}_{\mathtt{pk}(sk_b)} , \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right) \right\|_{m\text{-enc}} = 1$$

$$\left\| \{(r, \mathtt{snd}((y, m)))\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\left\| \left\{ \left(r, \mathtt{snd}\left(\mathtt{dec}\left(\{(y, m)\}_{\mathtt{pk}(sk_b)} , sk_b \right) \right) \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} =$$

$$\|(a, b)\|_{m\text{-enc}} =$$

Encryption as measure of secrecy

We define the *encryption level of m in N*, as the minimum number of encryption levels the attacker cannot bypass in which the message m is nested in N (∞ if m does not occurs in N).

$$\left\|\{(a,m)\}_{\mathrm{pk}(sk_b)}\right\|_{m\text{-enc}} = 1 \qquad \left\|\left\{\left(a,\{m\}_{\mathrm{pk}(sk_b)}\right)\right\}_{\mathrm{pk}(sk_b)}\right\|_{m\text{-enc}} = 2$$

$$\left\|\left(\{(a,m)\}_{\mathrm{pk}(sk_b)},\left\{\left(a,\{m\}_{\mathrm{pk}(sk_b)}\right)\right\}_{\mathrm{pk}(sk_b)}\right)\right\|_{m\text{-enc}} = 1$$

$$\left\|\{(r,\mathrm{snd}((y,m)))\}_{\mathrm{pk}(sk_b)}\right\|_{m\text{-enc}} = 1$$

$$\left\|\left\{\left(r,\mathrm{snd}\left(\mathrm{dec}\left(\{(y,m)\}_{\mathrm{pk}(sk_b)},sk_b\right)\right)\right)\right\}_{\mathrm{pk}(sk_b)}\right\|_{m\text{-enc}} = 1$$

(since $\left\{\left(r,\mathrm{snd}\left(\mathrm{dec}\left(\{(y,m)\}_{\mathrm{pk}(sk_b)},sk_b\right)\right)\right)\right\}_{\mathrm{pk}(sk_b)} \to_{\mathsf{E}} \{(r,\mathrm{snd}((y,m)))\}_{\mathrm{pk}(sk_b)}$)

$$\|(a,b)\|_{m\text{-enc}} =$$

Encryption as measure of secrecy

We define the *encryption level of m in N*, as the minimum number of encryption levels the attacker cannot bypass in which the message m is nested in N (∞ if m does not occurs in N).

$$\left\| \{(a,m)\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 1 \qquad \left\| \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 2$$

$$\left\| \left(\{(a,m)\}_{\mathtt{pk}(sk_b)}, \left\{ \left(a, \{m\}_{\mathtt{pk}(sk_b)} \right) \right\}_{\mathtt{pk}(sk_b)} \right) \right\|_{m\text{-enc}} = 1$$

$$\left\| \{(r, \mathtt{snd}((y,m)))\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 1$$

$$\left\| \left\{ \left(r, \mathtt{snd}\left(\mathtt{dec}\left(\{(y,m)\}_{\mathtt{pk}(sk_b)}, sk_b \right) \right) \right) \right\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} = 1$$

(since $\left\{ \left(r, \mathtt{snd}\left(\mathtt{dec}\left(\{(y,m)\}_{\mathtt{pk}(sk_b)}, sk_b \right) \right) \right) \right\}_{\mathtt{pk}(sk_b)} \to_E \{(r, \mathtt{snd}((y,m)))\}_{\mathtt{pk}(sk_b)}$)

$$\|(a,b)\|_{m\text{-enc}} = \infty$$

A simple useful result

Lemma

Let Γ be the list of the messages known by the attacker e during the execution of the DY3 *protocol. If $\|X\|_{m\text{-enc}} > 0$ for all $X \in \Gamma$ and $sk_b \notin \Gamma$, then $\Gamma \vdash Y$ is provable only if $\|Y\|_{m\text{-enc}} > 0$.*

$$\frac{}{\text{fresh } \vec{x}; \Gamma, M \vdash M}\ (\textsc{Ax}) \qquad \frac{z \text{ fresh for } \vec{x}}{\text{fresh } \vec{x}; \Gamma \vdash z}\ (\textsc{Sol})$$

$$\frac{\text{fresh } \vec{x}; \Gamma \vdash M \quad \text{fresh } \vec{x}; \Gamma \vdash N}{\text{fresh } \vec{x}; \Gamma \vdash (M, N)}\ (\textsc{I-pair}) \qquad \frac{\text{fresh } \vec{x}; \Gamma \vdash M \quad \text{fresh } \vec{x}; \Gamma \vdash K}{\text{fresh } \vec{x}; \Gamma \vdash \{M\}_K}\ (\textsc{I-enc}) \qquad \frac{\text{fresh } \vec{x}; \Gamma \vdash K}{\text{fresh } \vec{x}; \Gamma \vdash \mathtt{pk}(K)}\ (\textsc{I-pk})$$

$$\frac{\text{fresh } \vec{x}; \Gamma, M, N \vdash K}{\text{fresh } \vec{x}; \Gamma, (M, N) \vdash K}\ (\textsc{E-pair}) \qquad \frac{\text{fresh } \vec{x}; \Gamma, M \vdash L \quad \text{fresh } \vec{x}; \Gamma \vdash K}{\text{fresh } \vec{x}; \Gamma, \{M\}_{\mathtt{pk}(K)} \vdash L}\ (\textsc{E-enc})$$

$$\frac{\text{fresh } \vec{x}; \Gamma, M \vdash L}{\text{fresh } \vec{x}; \Gamma, \mathtt{dec}\left(\{M\}_{\mathtt{pk}(K)}, K\right) \vdash L}\ (\textsc{E-dec}) \qquad \frac{\text{fresh } \vec{x}; \Gamma \vdash M \quad \text{fresh } \vec{x}; \Gamma \vdash K}{\text{fresh } \vec{x}; \Gamma \vdash \mathtt{dec}(M, K)}\ (\textsc{I-dec})$$

Sessions with the responder are not insightful

The knolwdge of an attacker e after intercepting the first message in a DY3 from a to b is the following:

$$\Gamma = \text{fresh}\, sk_a, sk_b, m; \mathtt{pk}(sk_a)\,, \mathtt{pk}(sk_b)\,, \{(a, m)\}_{\mathtt{pk}(sk_b)}$$

which satisfies the hypothesis of the lemma we proved.

Sessions with the responder are not insightful

The knolwdge of an attacker e after intercepting the first message in a DY3 from a to b is the following:

$$\Gamma = \text{fresh}\, sk_a, sk_b, m; \mathtt{pk}(sk_a)\,, \mathtt{pk}(sk_b)\,, \{(a, m)\}_{\mathtt{pk}(sk_b)}$$

which satisfies the hypothesis of the lemma we proved.

We know that in to reveal the secret m, we have to be able to perform a transition $\xrightarrow{\text{secret}(m)}$ which requires to be able to prove the sequent $\Gamma \vdash m$.

Sessions with the responder are not insightful

The knolwdge of an attacker e after intercepting the first message in a DY3 from a to b is the following:

$$\Gamma = \text{fresh}\, sk_a, sk_b, m; \mathtt{pk}(sk_a)\,, \mathtt{pk}(sk_b)\,, \{(a, m)\}_{\mathtt{pk}(sk_b)}$$

which satisfies the hypothesis of the lemma we proved.

We know that in to reveal the secret m, we have to be able to perform a transition $\xrightarrow{\text{secret}(m)}$ which requires to be able to prove the sequent $\Gamma \vdash m$.

... but $\|m\|_{m\text{-enc}} = 0$.

Sessions with the responder are not insightful

What if we use multiple session with the Responder?

Sessions with the responder are not insightful

What if we use multiple session with the Responder?

By sending (as attacker) a message of the shape

message attacker sends b	b's response
$\{(a, X)\}_{\mathtt{pk}(sk_b)}$	$\{(b, X)\}_{\mathtt{pk}(sk_a)}$
$\{(e, Y)\}_{\mathtt{pk}(sk_b)}$	$\{(b, Y)\}_{\mathtt{pk}(sk_e)}$

Sessions with the responder are not insightful

What if we use multiple session with the Responder?

By sending (as attacker) a message of the shape

message attacker sends b	b's response
$\{(a, X)\}_{\mathtt{pk}(sk_b)}$	$\{(b, X)\}_{\mathtt{pk}(sk_a)}$
$\{(e, Y)\}_{\mathtt{pk}(sk_b)}$	$\{(b, Y)\}_{\mathtt{pk}(sk_e)}$

But $\left\|\{(a, X)\}_{\mathtt{pk}(sk_b)}\right\|_{m\text{-enc}} > 1$ and

$$\left\|\{(b, Y)\}_{\mathtt{pk}(sk_e)}\right\|_{m\text{-enc}} = \|(b, Y)\|_{m\text{-enc}} = \|Y\|_{m\text{-enc}}$$

Sessions with the responder are not insightful

What if we use multiple session with the Responder?

By sending (as attacker) a message of the shape

message attacker sends b	b's response
$\{(a, X)\}_{\mathtt{pk}(sk_b)}$	$\{(b, X)\}_{\mathtt{pk}(sk_a)}$
$\{(e, Y)\}_{\mathtt{pk}(sk_b)}$	$\{(b, Y)\}_{\mathtt{pk}(sk_e)}$

But $\left\| \{(a, X)\}_{\mathtt{pk}(sk_b)} \right\|_{m\text{-enc}} > 1$ and

$$\left\| \{(b, Y)\}_{\mathtt{pk}(sk_e)} \right\|_{m\text{-enc}} = \|(b, Y)\|_{m\text{-enc}} = \|Y\|_{m\text{-enc}}$$

Since Y is a previous knowledge of the attacker, by coinduction we know that $\|Y\|_{m\text{-enc}} > 1$.

Sessions with the initiator are not insightful neither!

What if we use multiple session with the Initiator?

Sessions with the initiator are not insightful neither!

What if we use multiple session with the Initiator?

Each message sent by the initiator is

either $\{(a, m)\}_{\mathtt{pk}(sk_b)}$ or $\{(a, m')\}_{\mathtt{pk}(sk_b)}$

Sessions with the initiator are not insightful neither!

What if we use multiple session with the Initiator?

Each message sent by the initiator is

$$\text{either } \{(a, m)\}_{\mathtt{pk}(sk_b)} \qquad \text{or } \{(a, m')\}_{\mathtt{pk}(sk_b)}$$

... unless a sends a message of the shape $\{(e, m)\}_{\mathtt{pk}(sk_b)}$ or $\{(a, m)\}_{\mathtt{pk}(sk_e)}$

Sessions with the initiator are not insightful neither!

What if we use multiple session with the Initiator?

Each message sent by the initiator is

$$\text{either } \{(a, m)\}_{\mathtt{pk}(sk_b)} \qquad \text{or } \{(a, m')\}_{\mathtt{pk}(sk_b)}$$

... unless a sends a message of the shape $\{(e, m)\}_{\mathtt{pk}(sk_b)}$ or $\{(a, m)\}_{\mathtt{pk}(sk_e)}$

But $\left\|\{(a, m)\}_{\mathtt{pk}(sk_b)}\right\|_{m\text{-enc}} = 1$ and $\left\|\{(a, m')\}_{\mathtt{pk}(sk_b)}\right\|_{m\text{-enc}} = \infty$

Secrecy claim in DY3 is true

The secret is exposed when we have a transition of the shape

$$\frac{m\theta =_{\mathsf{E}} M}{[\theta,\ \mathrm{secret}(M)] \xrightarrow{\mathrm{secret}(m)} [\theta,\ 0]}\ (\textsc{Secret})$$

Secrecy claim in DY3 is true

The secret is exposed when we have a transition of the shape

$$\frac{m\theta =_{\mathsf{E}} M}{[\theta,\ \mathrm{secret}(M)] \xrightarrow{\mathrm{secret}(m)} [\theta,\ 0]}\ (\textsc{Secret})$$

which requires that we are able to prove $\Gamma \vdash m$ where Γ is the knowledge of the attacker

Secrecy claim in DY3 is true

The secret is exposed when we have a transition of the shape

$$\frac{m\theta =_{\mathsf{E}} M}{[\theta,\ \mathrm{secret}(M)] \xrightarrow{\mathrm{secret}(m)} [\theta,\ 0]}\ (\textsc{Secret})$$

which requires that we are able to prove $\Gamma \vdash m$ where Γ is the knowledge of the attacker

- all possible messages sent by a have measure > 0;
- all possible messages sent by b responding to a have measure > 0;
- all possible messages sent by b responding the attacker faking to be a have measure > 0;
- all possible messages sent b to the attacker making use of its knowledge have measure > 0;

We conclude by our lemma since $\|\Gamma\|_{m\text{-enc}} > 0$ and $\|m\|_{m\text{-enc}} = 0$.

Where we are

- We now have all the tools needed to describe attacks.
- We know that we have assumptions on the network matters.
- We now know how to disprove and prove a secrecy claim.
- What about other security properties?