Distributive encryption

A Baskar (CMI)   R Ramanujam (IMSc)   S P Suresh (CMI)

Automata, Concurrency, and Timed Systems
CMI
January 28, 2011

Outline

1. Introduction
2. The Dolev-Yao model
3. Size lower bounds
4. Complexity lower bound
5. Proof normalization
6. Upper bound proofs

Outline

Cryptographic operations – viewed logically

- Encryption is used to hide information

$$\frac{t \quad k}{\{t\}_k}\ encrypt$$

- Decryption requires the corresponding inverse key

$$\frac{\{t\}_k \quad inv(k)}{t}\ decrypt$$

- Want to bundle some data together? Concatenate them!

$$\frac{t_1 \quad t_2}{(t_1, t_2)}\ pair$$

- You can split a bundle anytime you want to

$$\frac{(t_0, t_1)}{t_i}\ split_i \ \ (i = 0, 1)$$

Cryptographic operations …

- Useful protocols can be built by composing these operations

$$A \rightarrow B : \{(id_A, n)\}_{pubk_B}$$
$$B \rightarrow A : \{n\}_{pubk_A}$$

- But we want more – for some applications like electronic voting
- Can A get B's signature on a note n, without revealing the contents to B?

Blind signatures

- A picks a random number r, and sends $[\{r\}_{pubk_B}, n]$ to B
- $[a, b]$ is a different kind of bundle – can be unbundled only by someone who has at least one of the components
- B signs the bundle – $\{[\{r\}_{pubk_B}, n]\}_{privk_B}$
- But magically the signature seeps through – $[r, \{n\}_{privk_B}]$
- There are implementations with all these properties – standard RSA encryption along with multiplication serving as the special bundling
- A receives the signed term and can retrieve $\{n\}_{privk_B}$ from it, since she has r

Blind pairs

- One can form blind pairs

$$\frac{t_1 \quad t_2}{[t_1, t_2]} \; blindpair$$

- One can unpack blind pairs, provided one of the components is already in one's possession

$$\frac{[t_0, t_1] \quad t_i\!\downarrow}{t_{1-i}} \; blindsplit_i$$

- All encryptions seep into blind pairs

$$\{[t, t']\}_k = [\{t\}_k, \{t'\}_k]$$

Outline

The basic model

$\dfrac{}{X \vdash t}\ Ax\ \ (t \in X)$	
$\dfrac{X \vdash (t_0, t_1)}{X \vdash t_i}\ split_i\ \ (i = 0, 1)$	$\dfrac{X \vdash t_0 \quad X \vdash t_1}{X \vdash (t_0, t_1)}\ pair$
$\dfrac{X \vdash \{t\}_k \quad X \vdash inv(k)}{X \vdash t}\ decrypt$	$\dfrac{X \vdash t \quad X \vdash k}{X \vdash \{t\}_k}\ encrypt$
destruction rules	construction rules

Figure: Derivation rules

Decidability

- The passive intruder deduction problem: given X and t, check if there is proof of $X \vdash t$
- This problem is decidable.
  - A notion of normal proofs.
  - If $X \vdash t$ is provable, there is a normal proof of $X \vdash t$.
  - Every term r occurring in a normal proof of $X \vdash t$ is a subterm of $X \cup \{t\}$.
  - Derive bounds on the size of normal proofs from this.

Non-normal proofs

- An example:

$$\dfrac{\dfrac{}{t}\,Ax \qquad \dfrac{}{t}\,Ax}{\dfrac{(t,t)}{t}\,split_0}\,pair$$

Non-normal proofs

- An example:

$$\dfrac{\dfrac{\dfrac{}{t}\,\mathit{Ax} \qquad \dfrac{}{t}\,\mathit{Ax}}{(t, t)}\,\mathit{pair}}{t}\,\mathit{split}_0$$

- Another one:

$$\dfrac{\dfrac{\dfrac{}{t}\,\mathit{Ax} \qquad \dfrac{}{k}\,\mathit{Ax}}{\{t\}_k}\,\mathit{encrypt} \qquad \dfrac{}{k}\,\mathit{Ax}}{t}\,\mathit{decrypt}$$

Normalization rules

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ \pi_1\\ t\end{array}\quad\begin{array}{c}\vdots\ \pi_2\\ t'\end{array}}{(t,t')}\,pair}{t}\,split_0 \quad\rightsquigarrow\quad \begin{array}{c}\vdots\ \pi_1\\ t\end{array}$$

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ \pi_1\\ t\end{array}\quad\begin{array}{c}\vdots\ \pi_2\\ k\end{array}}{\{t\}_k}\,pair\qquad\begin{array}{c}\vdots\ \pi_3\\ inv(k)\end{array}}{t}\,decrypt \quad\rightsquigarrow\quad \begin{array}{c}\vdots\ \pi_1\\ t\end{array}$$

Subterm property

Lemma

If π is a normal proof of $X \vdash t$ and r occurs in π:

- $r \in st(X \cup \{t\})$
- *if π ends in a destruction rule, then $r \in st(X)$.*

Subterm property

Lemma

If π is a normal proof of $X \vdash t$ and r occurs in π:

- $r \in st(X \cup \{t\})$
- *if π ends in a destruction rule, then $r \in st(X)$.*

$$\dfrac{\begin{array}{cc} \vdots\,\pi_1 & \vdots\,\pi_2 \\ t & k \end{array}}{\{t\}_k}\ \mathit{encrypt}$$

- if r occurs in π_1,
  $r \in st(X \cup \{t\})$
- if r occurs in π_2,
  $r \in st(X \cup \{k\})$
- therefore, if r occurs in π,
  $r \in st(X \cup \{\{t\}_k\})$

Subterm property

Lemma

If π is a normal proof of $X \vdash t$ and r occurs in π:

- $r \in st(X \cup \{t\})$
- *if π ends in a destruction rule, then* $r \in st(X)$.

$$\dfrac{\begin{matrix}\vdots\,\pi_1 \\ \{t\}_k\end{matrix} \qquad \begin{matrix}\vdots\,\pi_2 \\ inv(k)\end{matrix}}{t}\,decrypt$$

- if r occurs in π_1 or π_2, $r \in st(X \cup \{\{t\}_k\})$
- since π is normal, π_1 does not end with the *encrypt* rule
- so it ends with a destruction rule, and $\{t\}_k \in st(X)$
- so any r occurring in π is in $st(X)$.

A polynomial-time algorithm

- The height of a normal proof of $X \vdash t$ is bounded by $n = |st(X \cup \{t\})|$.
- Let $X_0 = X$
- Compute $X_i = \text{one-step-derivable}(X_{i-1}) \cap st(X \cup \{t\})$, for $i \leq n$
- Check if $t \in X_n$!

Distributive encryption in Dolev-Yao

$$\mathscr{T} ::= m \mid (t_1, t_2) \mid [t_1, t_2] \mid \{t\}_k$$

Normal terms: Terms that do not contain a subterm of the form $\{[t_1, t_2]\}_k$.
For a term t, get its normal form $t{\downarrow}$ by pushing encryptions over blind pairs, all the way inside.

Distributive encryption in Dolev-Yao

$$\mathscr{T} \ ::= \ m \mid (t_1, t_2) \mid [t_1, t_2] \mid \{t\}_k$$

Normal terms: Terms that do not contain a subterm of the form $\{[t_1, t_2]\}_k$. For a term t, get its normal form $t{\downarrow}$ by pushing encryptions over blind pairs, all the way inside.

$\dfrac{[t, t'] \quad k}{[\{t\}_k{\downarrow}, \{t\}_k{\downarrow}]}\ \mathit{encrypt}$	$\dfrac{\{t\}_k{\downarrow} \quad \mathit{inv}(k)}{t}\ \mathit{decrypt}$	$\dfrac{(t_0, t_1)}{t_i}\ \mathit{split}_i$	$\dfrac{[t_0, t_1]{\downarrow} \quad t_i{\downarrow}}{t_{1-i}}\ \mathit{blindsplit}_i$
$\dfrac{}{t}\ \mathit{Ax} \ \ (t \in X)$	$\dfrac{t \quad k}{\{t\}_k{\downarrow}}\ \mathit{encrypt}$	$\dfrac{t_1 \quad t_2}{(t_1, t_2)}\ \mathit{pair}$	$\dfrac{t_1 \quad t_2}{[t_1, t_2]}\ \mathit{blindpair}$

Figure: analz and synth rules for normal terms (with assumptions from $X \subseteq \mathscr{T}$)

Alternative theories

- A simpler system. Delaune, Kremer, Ryan 2009, Baskar, Ramanujam, Suresh 2007.

$$\frac{[t, \{m\}_k] \quad inv(k)}{[\{t\}_{inv(k)}, m]}$$

  Passive intruder deduction is ptime decidable.

- A much harder system. Lafourcade, Lugiez, Treinen 2007.

$$\frac{t_1 + \cdots + t_\ell \quad k}{\{t_1\}_k + \cdots + \{t_\ell\}_k}$$

$$\frac{t_1 + \cdots + t_\ell + \cdots + t_m \quad t_\ell + \cdots + t_m + \cdots + t_n}{t_1 + \cdots + t_{\ell-1} - t_{m+1} - \cdots - t_n}$$

  Decidable but non-elementary upper bound.

- Our system: Decidable with a dexptime upper bound and a dexptime lower bound.

Related work

- What about other cryptographic primitives?
- Diffie-Hellman encryption, exclusive or, homomorphic encryption, blind signatures, …
- A large body of results: Rusinowitch & Turuani 2003, Millen & Shmatikov 2001, Comon & Shmatikov 2003, Chevalier, Küsters, Rusinowitch & Turuani 2005, Delaune & Jacquemard 2006, Bursuc, Comon & Delaune 2007
- But distributive encryption is an especially hard case that is not subsumed by these theories

Outline

No subterm property!

$$\dfrac{\dfrac{\dfrac{}{[a,b]}\,\mathit{Ax} \qquad \dfrac{}{k}\,\mathit{Ax}}{[\{a\}_k,\{b\}_k]}\,\mathit{encrypt} \qquad \dfrac{}{\{b\}_k}\,\mathit{Ax}}{\{a\}_k}\,\mathit{blindsplit}_1$$

Proof size lower bounds

Theorem

For every n, there exist X_n, t_n such that:

1. $size(X_n, t_n)$ *is* $O(n)$
2. $X_n \vdash t_n$
3. *Any proof of* $X_n \vdash t_n$ *is of size at least* 2^n.

Exponential size proof

- $K = \{k, k', k_0, k_1\}$. 0 will denote k_0, 1 will denote k_1
- $\underline{m}$ is the reverse of the n-bit representation of $m \in \{0, \ldots, 2^n - 1\}$
- X_0 is the following set:

$$\{a\}_{k\underline{0}k'}$$

$$[\{b_1\}_0, a], [\{b_2\}_0, b_1], \ldots, [\{b_n\}_0, b_{n-1}]$$

$$[\{b_1\}_1, a], [\{b_2\}_1, b_1], \ldots, [\{b_n\}_1, b_{n-1}]$$

$$[\{a\}_k, b_n], [\{c\}_{\underline{2^n-1}}, a]$$

- The following sequent can be derived:

$$X_0, K \vdash \{c\}_{\underline{2^n-1}k\underline{i_r}k\cdots k\underline{i_0}k\underline{0}k'}$$

Exponential size proof ...

- X_1 is the following set (where ℓ ranges over $\{k_0, k_1, k\}$:

$$\{e\}_{k'}, [\{e\}_\ell, e]$$

$$[\{g_0\}_0, e], [\{g_1\}_\ell, g_0], \ldots, [\{g_{n+1}\}_\ell, g_n]$$

$$[\{f_0\}_1, e], [\{f_1\}_\ell, f_0], \ldots, [\{f_{n+1}\}_\ell, f_n]$$

- The following derivations are possible, where $x, y \in \{k, k_0, k_1\}^*, |y| = n + 1$:

$$X_1, K \vdash \{e\}_{xk\underline{0}k'}$$

$$X_1, K \vdash \{g_n\}_{y0xk\underline{0}k'}$$

$$X_1, K \vdash \{f_n\}_{y1xk\underline{0}k'}$$

- X_2 is the following set :

$$[[c, \{c\}_0], f_n], [[d, \{c\}_1], g_n]$$

$$[[d, \{d\}_0], g_n], [[d, \{d\}_1], f_n]$$

- The following derivation is possible:

$$X_1, X_2, K, \{c\}_{\underline{i+1}k\underline{i}xk'} \vdash \{c\}_{\underline{i}xk'}$$

Exponential size proof ...

- X_2 is the following set :

$$[[c, \{c\}_0], f_n], [[d, \{c\}_1], g_n]$$

$$[[d, \{d\}_0], g_n], [[d, \{d\}_1], f_n]$$

- The following derivation is possible:

$$X_1, X_2, K, \{c\}_{\underline{i+1}k\underline{i}xk'} \vdash \{c\}_{\underline{i}xk'}$$

- To prevent accidental decryptions, we actually take X_2 to be:

$$[[[[c, \{c\}_0], f_n], \{c\}_0], f_n], [[d, \{c\}_1], g_n], \{c\}_1], g_n], \ldots$$

Exponential size proof …

- $X = X_0 \cup X_1 \cup X_2 \cup K$
- $X \vdash \{c\}_{\underline{0}k'}$
- One can also prove that every derivation of the above contains the term $\{c\}_{\underline{2^n - 1}k\underline{i_r}k \cdots k\underline{i_0}k\underline{0}k'}$, but arbitrary derivations are hard to analyze!
- Strategy: Show that every proof can be transformed to a normal proof without introducing new terms in the proof, and analyze normal proofs.

Outline

Alternating pushdown systems

Definition

An **alternating pushdown system** is a triple $\mathscr{P} = (P, \Gamma, \hookrightarrow)$ where:

- P is a *finite set of control locations*,
- Γ is a *finite stack alphabet*,
- and $\hookrightarrow \subseteq P \times \Gamma^* \times 2^{(P \times \Gamma^*)}$ is a *finite set of transition rules*.

Transitions are written $(a, x) \hookrightarrow \{(b_1, x_1), \ldots, (b_n, x_n)\}$.

Definition

A *configuration* is a pair (a, x) where $a \in P$ and $x \in \Gamma^*$. Given a set of configurations C, a configuration (a, x), and $i \geq 0$, we say that $(a, x) \Rightarrow_{\mathscr{P},i} C$ iff:

- $(a, x) \in C$ and $i = 0$, or
- there is a transition $(a, y) \hookrightarrow \{(b_1, y_1), \ldots, (b_n, y_n)\}$ of $\mathscr{P}$, $z \in \Gamma^*$, and $i_1, \ldots, i_n$ such that $i = i_1 + \cdots + i_n + 1$ and $x = yz$ and $(b_j, y_j z) \Rightarrow_{\mathscr{P},i_j} C$ for all $j \in \{1, \ldots, n\}$.

We say that $(a, x) \Rightarrow_{\mathscr{P}} C$ iff $(a, x) \Rightarrow_{\mathscr{P},i} C$ for some $i \geq 0$.

Alternating pushdown systems …

Theorem (Suwimonteerabuth, Schwoon, Esparza 2006)

The **backwards-reachability problem for alternating pushdown systems**, *which asks, given an APDS* $\mathscr{P}$ *and configurations* (s, x_s) *and* (f, x_f), *whether* $(s, x_s) \Rightarrow_{\mathscr{P}} (f, x_f)$, *is* DEXPTIME-*complete.*

Given an APDS $\mathscr{P} = (P, \Gamma, \hookrightarrow)$, with rules in $\hookrightarrow$ are numbered 1 to ℓ and two configurations (s, x_s) and (f, x_f).
Take $M = P \cup \{\mathbf{c}_m \mid 1 \leq m \leq \ell\}$ to be a set of atomic terms, and $K = \Gamma \cup \{d, e\}$ to be a set of *non-symmetric keys*.
Suppose the m^{th} rule is:

$$(a, x) \hookrightarrow \{(b_1, x_1), \ldots, (b_n, x_n)\}$$

This gets translated to the following term $\mathbf{r}_m$:

$$\mathbf{r}_m = [[\cdots[[\mathbf{r}'_m, \{b_1\}_{x_1}], \{b_2\}_{x_2}], \cdots, \{b_{n-1}\}_{x_{n-1}}], \{b_n\}_{x_n}], \text{ where}$$
$$\mathbf{r}'_m = [[\cdots[[\{\mathbf{c}_m\}_d, \{a\}_x], \{b_1\}_{x_1}], \cdots, \{b_{n-1}\}_{x_{n-1}}], \{b_n\}_{x_n}].$$

The reduction ...

We take X to be the set
$\{\mathbf{r}_m \mid 1 \leq m \leq \ell\} \cup \{\{f\}_{x_f e}\} \cup \{\{\mathbf{c}_m\}_d \mid 1 \leq m \leq \ell\} \cup \Gamma \cup \{e\}$.

Theorem

$(s, x_s) \Rightarrow_{\mathscr{P}} (f, x_f)$ *iff* $X \vdash \{s\}_{x_s e}$.

Theorem

The passive intruder deduction problem is dexptime-hard.

Outline

Proof normalization

$$\dfrac{\dfrac{\overset{\vdots\;\pi'}{t'} \qquad \overset{\vdots\;\pi''}{t''}}{[t', t'']}\;\mathit{blindpair} \qquad \overset{\vdots\;\delta}{k}}{[\{t'\}_{k\downarrow}, \{t''\}_{k\downarrow}]}\;\mathit{encrypt}$$

$$\dfrac{\dfrac{\overset{\vdots\;\pi'}{t'} \qquad \overset{\vdots\;\delta}{k}}{\{t'\}_{k\downarrow}}\;\mathit{encrypt} \qquad \dfrac{\overset{\vdots\;\pi''}{t''} \qquad \overset{\vdots\;\delta}{k}}{\{t''\}_{k\downarrow}}\;\mathit{encrypt}}{[\{t'\}_{k\downarrow}, \{t''\}_{k\downarrow}]}\;\mathit{blindpair}$$

$$\dfrac{\dfrac{\overset{\vdots\;\pi'}{\{t'\}_{k\downarrow}} \qquad \overset{\vdots\;\pi''}{\{t''\}_{k\downarrow}}}{[\{t'\}_{k\downarrow}, \{t''\}_{k\downarrow}]}\;\mathit{blindpair} \qquad \overset{\vdots\;\delta}{\mathit{inv}(k)}}{[t', t'']}\;\mathit{decrypt}$$

$$\dfrac{\dfrac{\overset{\vdots\;\pi'}{\{t'\}_{k\downarrow}} \qquad \overset{\vdots\;\delta}{\mathit{inv}(k)}}{t'}\;\mathit{decrypt} \qquad \dfrac{\overset{\vdots\;\pi''}{\{t''\}_{k\downarrow}} \qquad \overset{\vdots\;\delta}{\mathit{inv}(k)}}{t''}\;\mathit{decrypt}}{[t', t'']}\;\mathit{blindpair}$$

Figure: The normalization rules I

Proof normalization …

$$\dfrac{\dfrac{\overset{\vdots\,\pi'}{[t,t']} \quad \overset{\vdots\,\pi''}{t'}}{t}\,\textit{blindsplit} \qquad \overset{\vdots\,\delta}{k}}{\{t\}_{k\downarrow}}\,\textit{encrypt}$$

$$\dfrac{\dfrac{\overset{\vdots\,\pi'}{[t,t']} \quad \overset{\vdots\,\delta}{k}}{[\{t'\}_{k\downarrow},\{t'\}_{k\downarrow}]}\,\textit{encrypt} \qquad \dfrac{\overset{\vdots\,\pi''}{t'} \quad \overset{\vdots\,\delta}{k}}{\{t'\}_{k\downarrow}}\,\textit{e}}{\{t\}_{k\downarrow}}\,\textit{blind}$$

$$\dfrac{\dfrac{\overset{\vdots\,\pi'}{[\{t'\}_{k\downarrow},\{t'\}_{k\downarrow}]} \quad \overset{\vdots\,\pi''}{\{t'\}_{k\downarrow}}}{\{t\}_{k\downarrow}}\,\textit{blindsplit} \qquad \overset{\vdots\,\delta}{inv(k)}}{t}\,\textit{decrypt}$$

$$\dfrac{\dfrac{\overset{\vdots\,\pi'}{[\{t'\}_{k\downarrow},\{t'\}_{k\downarrow}]} \quad \overset{\vdots\,\delta}{inv(k)}}{[t,t']}\,\textit{decrypt} \qquad \dfrac{\overset{\vdots\,\pi''}{\{t'\}_{k\downarrow}} \quad \textit{in}}{t'}}{t}\,\textit{blin}$$

Figure: The normalization rules II

Proof normalization …

Lemma

Whenever $X \vdash t$*, there is a normal proof of* t *from* X*.*

Proof normalization ...

Lemma

Whenever $X \vdash t$*, there is a normal proof of* t *from* X.

Lemma

Let π *be a normal proof of* t *from* X*, and let* δ *be a sub-proof of* π *with root labelled* r*. Then the following hold:*

1. *If* δ *ends with an* analz *rule, then for every* u *occurring in* δ *there is* $p \in st(X)$ *and keyword* x *such that* $u = \{p\}_x\downarrow$.
2. *If* δ *ends with a* synth *rule, then for every* u *occurring in* δ*, either* $u \in st(X \cup \{r\})$ *or there is* $p \in st(X)$ *and keyword* x *such that* $u = \{p\}_x\downarrow$.
3. *If the last rule of* δ *is decrypt or split with major premise* r_1*, then* $r_1 \in st(X)$.

Outline

Decidability: the proof idea

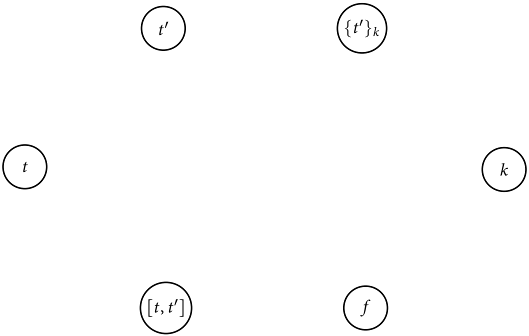
- Show that every term in a normal proof of $X \vdash t$ is of the form $\{p\}_x$ where $p \in st(X \cup \{t\})$ and x is a sequence of keys from $st(X \cup \{t\})$.
- Show that for each $p \in st(X \cup \{t\})$, $\mathscr{L}_p = \{x \in \mathscr{K}^* | X \vdash \{p\}_x\}$ is a regular set.
- To check whether $X \vdash t$, check whether $\varepsilon \in \mathscr{L}_t$.

Decidability: the proof idea

- Show that every term in a normal proof of $X \vdash t$ is of the form $\{p\}_x$ where $p \in st(X \cup \{t\})$ and x is a sequence of keys from $st(X \cup \{t\})$.
- Show that for each $p \in st(X \cup \{t\})$, $\mathscr{L}_p = \{x \in \mathscr{K}^* | X \vdash \{p\}_x\}$ is a regular set.
- To check whether $X \vdash t$, check whether $\varepsilon \in \mathscr{L}_t$.
- Properties of the $\mathscr{L}_p$:
  - $kx \in \mathscr{L}_p$ iff $x \in \mathscr{L}_{\{p\}_k}$
  - if $x \in \mathscr{L}_p$ and $x \in \mathscr{L}_{[p,p']}$, then $x \in \mathscr{L}_{p'}$
  - if $x \in \mathscr{L}_p$ and $\varepsilon \in \mathscr{L}_k$, then $xk \in \mathscr{L}_p$
  - if $\varepsilon \in \{t\}_k$ and $\varepsilon \in inv(k)$ then $\varepsilon \in t$.

An example

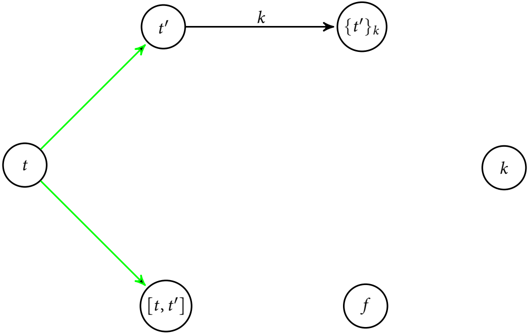
$$\{[t, t'], \{t'\}_k, k\} \vdash \{t\}_k$$



the set of subterms

An example

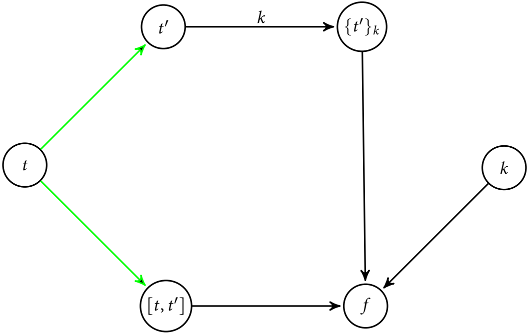
$$\{[t, t'], \{t'\}_k, k\} \vdash \{t\}_k$$



$t', [t, t'] \vdash t$ and t' encrypted with k is $\{t'\}_k$

An example

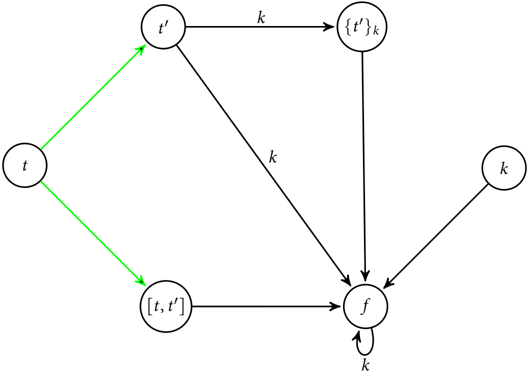
$\{[t, t'], \{t'\}_k, k\} \vdash \{t\}_k$



the initial set of terms X

An example

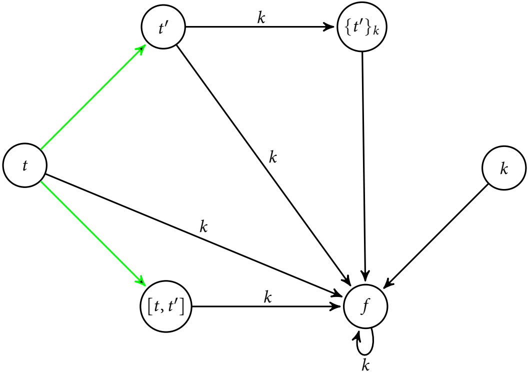
$$\{[t, t'], \{t'\}_k, k\} \vdash \{t\}_k$$



$k \in X$ and $t' \overset{k}{\Rightarrow} f$

An example

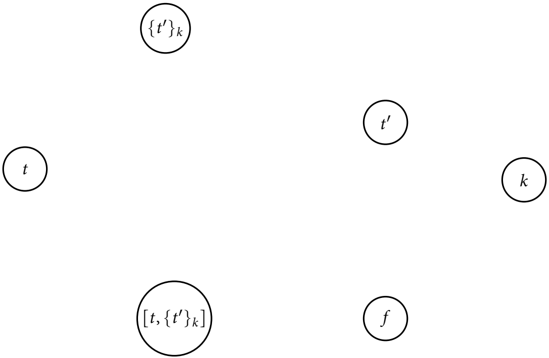
$$\{[t,t'],\{t'\}_k,k\} \vdash \{t\}_k$$



$[t,t'] \overset{k}{\Rightarrow} f$ and $t \overset{k}{\Rightarrow} f$

Another example

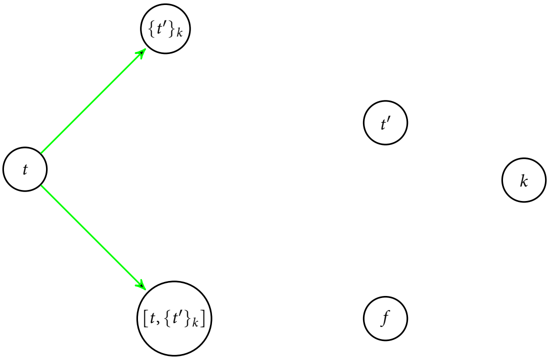
$$\{[t, \{t'\}_k], t', k\} \vdash t$$



the set of subterms

Another example

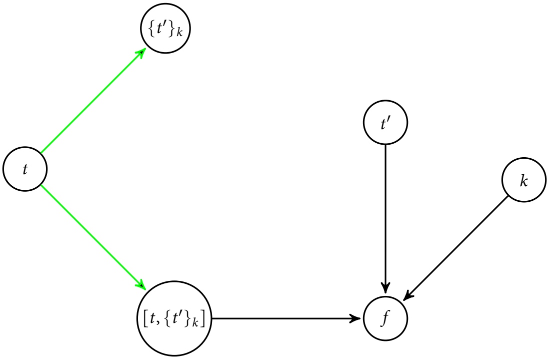
$\{[t, \{t'\}_k], t', k\} \vdash t$



$\{t'\}_k, [t, \{t'\}_k] \vdash t$

Another example

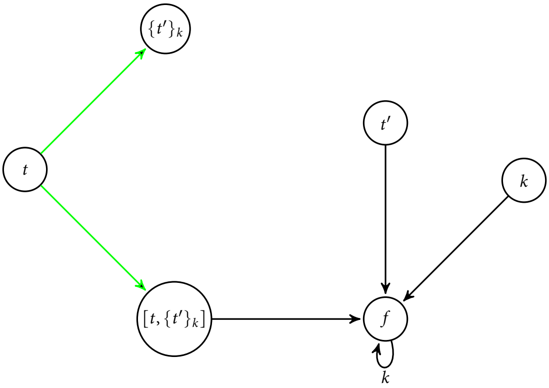
$$\{[t, \{t'\}_k], t', k\} \vdash t$$



the initial set of terms X

Another example

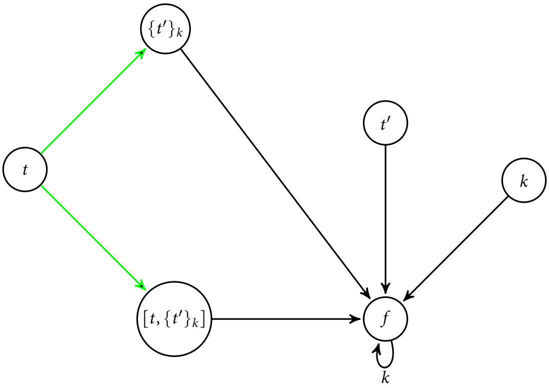
$$\{[t, \{t'\}_k], t', k\} \vdash t$$



$k \in X$

Another example

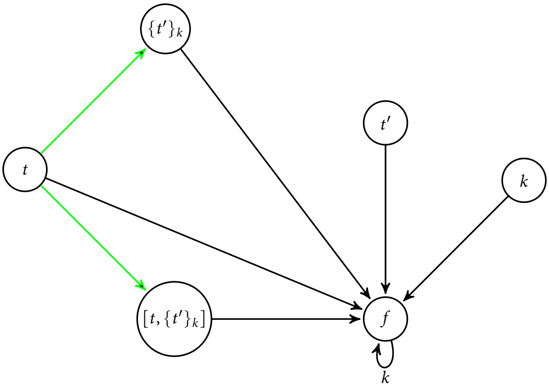
$$\{[t, \{t'\}_k], t', k\} \vdash t$$



$$t' \overset{k}{\Rightarrow} f$$

Another example

$$\{[t, \{t'\}_k], t', k\} \vdash t$$



$t \Rightarrow f$

The automaton construction

Similar to the construction in [Bouajjani, Esparza, Maler 1997]

$$\mathscr{A}_i = (Q, \Sigma, \hookrightarrow_i, F),\ Q = Y_0 \cup \{f\},\ \Sigma = K_0, \text{ and } F = \{f\}.$$

The automaton construction

Similar to the construction in [Bouajjani, Esparza, Maler 1997]

$$\mathscr{A}_i = (Q, \Sigma, \hookrightarrow_i, F),\ Q = Y_0 \cup \{f\},\ \Sigma = K_0, \text{ and } F = \{f\}.$$

- 1. if $t \in Y_0$, $k \in K_0$ such that $\{t\}_k\!\downarrow \in Y_0$, then $t \overset{k}{\hookrightarrow}_0 \{\{t\}_k\!\downarrow\}$.
  2. if $t, t', t'' \in Y_0$ such that t is the conclusion of an instance of the *blindpair* or *blindsplit*$_i$ rules with premises t' and t'', then $t \overset{\varepsilon}{\hookrightarrow}_0 \{t', t''\}$.

The automaton construction

Similar to the construction in [Bouajjani, Esparza, Maler 1997]

$\mathscr{A}_i = (Q, \Sigma, \hookrightarrow_i, F)$, $Q = Y_0 \cup \{f\}$, $\Sigma = K_0$, and $F = \{f\}$.

- 1. if $t \in Y_0$, $k \in K_0$ such that $\{t\}_k\!\downarrow \in Y_0$, then $t \overset{k}{\hookrightarrow}_0 \{\{t\}_k\!\downarrow\}$.
  2. if $t, t', t'' \in Y_0$ such that t is the conclusion of an instance of the *blindpair* or *blindsplit*$_i$ rules with premises t' and t'', then $t \overset{\varepsilon}{\hookrightarrow}_0 \{t', t''\}$.

- 1. if $q \overset{a}{\Rightarrow}_i C$, then $q \overset{a}{\hookrightarrow}_{i+1} C$.
  2. if $\{t\}_k\!\downarrow \in Y_0$ and $t \overset{k}{\Rightarrow}_i C$, then $\{t\}_k\!\downarrow \overset{\varepsilon}{\hookrightarrow}_{i+1} C$.
  3. if $k \in K_0$ and $k \overset{\varepsilon}{\Rightarrow}_i \{f\}$, then $f \overset{k}{\hookrightarrow}_{i+1} \{f\}$.
  4. if $\Gamma \subseteq Y_0$, $t \in Y_0$, and if there is an instance **r** of one of the rules whose set of premises is (exactly) Γ and conclusion is t the following holds:

$$\text{if } u \overset{\varepsilon}{\Rightarrow}_i \{f\} \text{ for every } u \in \Gamma,\ \text{then } t \overset{\varepsilon}{\hookrightarrow}_{i+1} \{f\}.$$

Correctness of the construction

Theorem

(**Completeness**) *For any* $t \in Y_0$ *and any keyword* x, *if* $X_0 \vdash \{t\}_x\downarrow$, *then there exists* $i \geq 0$ *such that* $t \overset{x}{\Rightarrow}_i \{f\}$.

Correctness of the construction

Theorem

(**Completeness**) *For any $t \in Y_0$ and any keyword x, if $X_0 \vdash \{t\}_x\downarrow$, then there exists $i \geq 0$ such that $t \overset{x}{\Rightarrow}_i \{f\}$.*

Lemma

Suppose $i, d \geq 0$, $t \in Y_0$, $x, y \in K_0^*$, and $C \subseteq Q$ (with $D = C \cap Y_0$). Suppose the following also hold: 1) $t \overset{x}{\Rightarrow}_{i,d} C$, and 2) $C \subseteq Y_0$ or $X_0 \vdash y$. Then $X_0 \cup \{D\}_y \vdash \{t\}_{xy}$.

Correctness of the construction

Theorem

*(**Completeness**) For any $t \in Y_0$ and any keyword x, if $X_0 \vdash \{t\}_x\downarrow$, then there exists $i \geq 0$ such that $t \overset{x}{\Rightarrow}_i \{f\}$.*

Lemma

Suppose $i, d \geq 0$, $t \in Y_0$, $x, y \in K_0^*$, and $C \subseteq Q$ (with $D = C \cap Y_0$). Suppose the following also hold: 1) $t \overset{x}{\Rightarrow}_{i,d} C$, and 2) $C \subseteq Y_0$ or $X_0 \vdash y$. Then $X_0 \cup \{D\}_y \vdash \{t\}_{xy}$.

Theorem

*(**Soundness**) For any i, any $t \in Y_0$, and any keyword x, if $t \overset{x}{\Rightarrow}_i \{f\}$, then $X_0 \vdash \{t\}_x\downarrow$.*

Theorem

The problem of checking whether $X \vdash t$, given X and t, is solvable in time $2^{O(n)}$, where n is the size of $X \cup \{t\})$.

Proof.

The automaton saturation procedure only adds transitions, and the total number of transitions possible is $2^{O(n)}$. Each refinement step takes time $2^{O(n)}$. □

Summary

- Interesting extension of the Dolev-Yao theory

Summary

- Interesting extension of the Dolev-Yao theory
- One of the very few lower bound results for the passive intruder deduction problem

Summary

- Interesting extension of the Dolev-Yao theory
- One of the very few lower bound results for the passive intruder deduction problem
- Both upper and lower bound proofs reveal interesting connections with some automata models

Summary

- Interesting extension of the Dolev-Yao theory
- One of the very few lower bound results for the passive intruder deduction problem
- Both upper and lower bound proofs reveal interesting connections with some automata models
- Results can be extended to systems which use constructed keys rather than atomic keys, and also systems which treat the blind pair operator to be associative.

Summary

- Interesting extension of the Dolev-Yao theory
- One of the very few lower bound results for the passive intruder deduction problem
- Both upper and lower bound proofs reveal interesting connections with some automata models
- Results can be extended to systems which use constructed keys rather than atomic keys, and also systems which treat the blind pair operator to be associative.
- Hard problem (yet to be tackled): Getting better upper bounds for the theory which considers an abelian group operator with distributive encryption, improving LLT2007.

Questions?

Thank you!