DECIDING STATIC INCLUSION FOR Δ-STRONG AND $\omega\nabla$-STRONG INTRUDER THEORIES:

APPLICATIONS TO CRYPTOGRAPHIC PROTOCOL ANALYSIS

by

Kimberly A. Gero

A Dissertation

Submitted to the University at Albany, State University of New York

in Partial Fulfillment of

the Requirements for the Degree of

Doctor of Philosophy

College of Computing and Information

Department of Computer Science

2015

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

DECIDING STATIC INCLUSION FOR Δ-STRONG AND $\omega\nabla$-STRONG INTRUDER THEORIES:

APPLICATIONS TO CRYPTOGRAPHIC PROTOCOL ANALYSIS

by

Kimberly A. Gero

To my parents

ABSTRACT

In this dissertation we will be studying problems relating to *indistinguishability*. This topic is of great interest and importance to cryptography. Cryptographic protocol analysis is currently being studied a great deal due to numerous high profile security breaches. The form of indistinguishability that we will be focusing on is *static inclusion* and its sub-case *static equivalence*. Our work in this dissertation is based on "Intruders with Caps." Our main results are providing co-saturation procedures for deciding whether a frame A is statically included in a frame B over Δ-strong and $\omega\triangledown$-strong intruder theories, where a frame consists of hidden data and substitutions that represent knowledge that an intruder could have gained from eavesdropping on message exchanges by agents.

ACKNOWLEDGMENTS

I would like to thank my advisor Dr. Paliath Narendran for his guidance and for taking me on as a PhD student. Dran always listens patiently to my ideas, is very supportive, and has provided me with lots of great feedback. I am also quite thankful for his accessibility throughout my time as his PhD student especially during the last few years when I was able to interrupt almost any meeting with questions.

I would like to thank my committee members Dr. Neil Murray and Dr. Christopher Lynch, who was also a very valuable co-author, for their advice, discussions and time. I would also like to thank Dr. Siva Anantharaman and Dr. Michael Rusinowitch for their invaluable feedback on this dissertation and the related papers we are currently writing. I would like to thank Dr. Catherine Meadows for giving me advice and guidance during my summer internship at the Naval Research Lab.

I am very thankful to Dr. Lonnie Fairchild for encouraging me to pursue a doctoral degree. She encouraged me to apply to a great program which helped me realize that I wanted to do research. Dr. Jan Plaza's advice and guidance on my Advanced Honors Project helped me develop research skills that enabled me to get where I am today. The research experience that I received in undergrad was very much due to Lonnie and Jan.

I also like to thank Dr. S. S. Ravi for providing me with lots of coffee and advice throughout my PhD. I would also like to thank Dr. Feng Chen for his valuable help with my teaching statement and CV. Additionally I would like to thank Dr. Mei-Hwa Chen for all of the advice she gave me as my academic advisor and for putting so much time into trying to improve my public speaking skills. I am also very grateful for the time that I got to spend getting to know Dr. Andrew Haas before his untimely passing. He always made lunch conversations very interesting and informative. I would like to thank Dr. Seth Chaiken for helping me practice for my defense.

I would like to thank Dr. Serdar Erbatur, Dr. Andrew Marshall and Christopher Bouchard for helping me get started in the Unification Group. Serdar's encouragement to join the group was a deciding factor in my decision to do protocol analysis. I am very grateful to Dr. Amanda Danko, Zumrut Akcam, Dan Hono, Dr. Andrew Matusiewicz,

Paul Olsen, and Peter Hibbs for giving me advice and friendship throughout my PhD. I would like to thank William Augustine for all of his help over the years and the much needed study breaks to discuss hockey. I would also like to thank the rest of the Unification group at UAlbany, my friends and my family.

I would like to thank my boyfriend Patrick Cornell for tolerating the long hours that I have put into writing this dissertation. He has always provided me with his love and support for the past seven years, even though when we started dating as undergraduates neither of us thought that I would decide to go for my PhD.

Finally, I would like to thank my parents Bonnie and Victor Gero for always supporting and strongly encouraging me in all of my dreams, especially academically. I never would have decided to pursue my PhD if my parents had not always supported my decisions.

CONTENTS

LIST OF FIGURES

CHAPTER 1
Introduction

Symbolic cryptographic protocol analysis is an important topic in cyber security, especially in the modern era. Recently we have seen many high profile security breaches in companies such as TARGET and SONY. Due to these and numerous other security exploitations, research in symbolic protocol analysis is emerging as a high priority.

Cryptographic protocols are designed to facilitate secure communication between agents. Communication is achieved through message exchanges in an environment that is, more often than not, hostile. Properties that are important in these exchanges are privacy (e.g., private data remains secret), authenticity (e.g., no spoofing attacks), and accessibility (e.g., no denial of service attacks). In our work we are mostly interested in privacy and authenticity.

1.1 Motivation and Contribution

In this dissertation we will be studying problems related to *indistinguishability*. Indistinguishability and related topics are currently being studied in many fields such as cyber security and data analytics (e.g., differential privacy). The indistinguishability problem asks if we are given two objects A and B is it possible to differentiate A from B. Some common examples of indistinguishability are the Turing test (e.g., can we distinguish between a human and an artificial intelligence?), zero knowledge proofs or protocols (e.g., can a third party observer determine if (s)he is witnessing a real or a fabricated run of the protocol?) and clinical trials (e.g., can the patient distinguish between receiving a placebo or the real drug? Can a medical researcher differentiate between the effect of the placebo and the real drug effect?). Indistinguishability is crucial when protecting low entropy data such as votes in electronic voting protocols where any loss of information can lead to loss of anonymity.

A common application of indistinguishability in cyber security is the detection of *guessing attacks*. An attack where an intruder makes a guess and is able to verify if the guess is correct is known as a guessing attack [29]. Guessing attacks are also known as

dictionary or brute force attacks. A guessing attack is offline when an attacker does not interact with other agents to verify his guess [20]. Some examples of protocols that were shown to be susceptible to offline guessing attacks are the Kerberos Authentication protocol [14], Peyravian-Jeffries's remote user authentication protocol [30], and the Encrypted Key Exchange (EKE) protocol [20].

The main topic that we shall be exploring in this dissertation is a property named static inclusion. We also look at static equivalence which can be viewed as a special case of static inclusion. Static equivalence is an interesting topic in cryptography since it has a significant relation to offline guessing attacks [13, 11, 21]. In [21] the authors show how to formulate guessing verification using static equivalence. Informally static equivalence can be illustrated using the following example with is based on the Dolev-Yao paper [25]:

Example 1.1.1. *Let Alice and Bob be agents that are trying to communicate in a hostile environment. Consider the following protocol:*

$$Alice \rightarrow Bob : \{M, N_1\}_k$$

$$Bob \rightarrow Alice : \{M, N_2\}_k$$

where M is a message, N_1 and N_2 are nonces (e.g., randomly generated strings) and k represents our potentially weak key. Consider an intruder Eve who has witnessed this message exchange tries to guess a value, k', for the key and decrypt the above message exchanges using k'. If Eve is then able to determine that the values for M are the same in both messages, then it is highly likely that her guess for k was correct.

We now look at this example in terms of substitutions. The messages witnessed by the intruder can be represented by the following substitution:

$$\theta \;=\; \{X_1 \rightarrow e(p(M, N_1), k),\; X_2 \rightarrow e(p(M, N_2), k)\}$$

where e represents the encryption operator and p represents pairing. In this example the set of hidden data contains M, N_1, N_2, k', and k.

Note that throughout this dissertation we will assume that cryptographic primitives are known to all agents including intruders. The intruder's capabilities can be represented

by a term rewriting system R as follows:

$$R \;=\; \{d(e(x,y),y) \to x,\; \pi_1(p(x,y)) \to x,\; \pi_2(p(x,y)) \to y\}$$

where the first rule represents the standard decryption operator, p is the pairing function, and π_i is the projection function on the i^{th} element where i is either 1 or 2.

Now suppose that the intruder wants to extend his knowledge by guessing a key k'. This can be viewed as an extension of θ:

$$\rho \;=\; \theta \cup \left\{X_3 \mapsto k'\right\}.$$

On the other hand, the principals know the correct key k, so their knowledge can be viewed as the substitution

$$\sigma \;=\; \theta \cup \{X_3 \mapsto k\}.$$

Clearly σ unifies the terms $\pi_1(d(X_1,X_3))$ and $\pi_1(d(X_2,X_3))$ modulo the rewrite system R, since it has the correct key whereas ρ does not.

Static equivalence can be viewed as a dual of the unification problem: here two substitutions are already given and the question is whether they unify the same terms over a given set of terms, namely the terms that the intruder can construct (called "recipes" in the literature). In the above example, the terms $\pi_1(d(X_1,X_3))$ and $\pi_1(d(X_2,X_3))$ are both recipes since the intruder can construct them with what he knows. Static inclusion, on the other hand, is the (asymmetric) question of whether ρ can unify every pair that σ can. Clearly static equivalence corresponds to the case where static inclusion holds both ways. We will formally define static inclusion and equivalence in Chapter 2.

Here is an example where there is no guessing attack, and thus static equivalence holds:

Example 1.1.2. *Consider the following protocol:*

$$Alice \to Bob : \{N_a\}_q$$

$$Bob \to Alice : \{M, N_a\}_K$$

where M is a message, N_a is a nonce, q represents our potentially weak key and K represents a strong key. [Note that this example is only for illustrative purposes and may not occur in practice since if Alice and Bob already had a strong key, they would not need to use a weak key q.]

Consider that an intruder *Eve* who has witnessed this message exchange tries to guess a value, q', for the weak key. As before, the intruder's capabilities are represented by the above term rewriting system R.

The set of hidden data in this example consists of M, N_a, q, q', and K. The substitutions we have this time are

$$\sigma = \{X_1 \mapsto e(N_a, q),\ X_2 \mapsto e(p(M, N_a), K),\ X_3 \mapsto q\}$$

and

$$\rho = \left\{X_1 \mapsto e(N_a, q),\ X_2 \mapsto e(p(M, N_a), K),\ X_3 \mapsto q'\right\}.$$

In this example static equivalence holds, therefore there does not exist a guessing attack. The intruder may be able to get N_a, but she will not be able to verify that her guess is correct since K cannot be guessed. We will discuss this example in Chapter 6.

Both static inclusion and static equivalence are very important problems in practice; however, static inclusion is somewhat rare in the literature. An application of static inclusion was studied in [17] where it was referred to as *static refinement.* Static inclusion is an undecidable problem in general, even for convergent term rewriting systems [1]. Our purpose in studying static inclusion is to identify decidable sub-cases.

Our approach can be seen as an extension to the approach given in "Intruders with Caps" [6]. In that paper the authors consider the *deduction problem* which is also known as the cap problem. Essentially what this problem asks is if we stack "cap" terms on top of the terms we are considering, can we gain access to the encrypted message? If we can get this message then we call the system treacherous or unsafe. Our approach is very closely based upon this paper. (The deduction problem is also undecidable for arbitrary convergent term rewriting systems [1].)

1.2 Related Work

Static inclusion and its sub-case static equivalence have been studied from many directions. Research has been going on in these and related problems for some time. Part of the reason why these types of problems have been studied so much is because humans tend to choose very poor and often easily guessable passwords [28].

Our approach to solving this problem is based on a saturation method. Some notation that we use is borrowed from the applied pi-calculus [2, 34], however no prior knowledge of it is required to understand our methodology. Our approach requires knowledge of term rewriting and syntactic unification. As this dissertation is being written, an alternative approach using a Knuth-Bendix [27] like completion procedure is also being developed [3, 31, 33]. That approach is related to ours and we will be incorporating both approaches into a paper.

Static equivalence decision procedures have been proposed for various equational theories [1, 22, 18] including subterm convergent theories. Yet Another Protocol Analysis Tool (YAPA) [12], Knowledge in Security protocols (KiSs) [23], and FAST [19] can verify static equivalence for a large set of equational theories; however the precise set of theories under which these algorithms terminate is not clear. ProVerif [15] is a general cryptographic protocol analysis tool that can verify equivalence properties even in presence of active attackers, but without termination guarantees.

Trace equivalence, a more general form of static equivalence, has been used to show that many protocols are in fact, insecure. One such protocol is Basic Access Control (BAC) that was used for French passport authentication [8, 16]. An interesting, and perhaps surprising, note is that this protocol became insecure due to the addition of certain security checks. When these checks were added the protocol's response time was not padded (i.e., successful and unsuccessful runs could have different run times). Thus if an adversary was able to time the response of various runs anonymity could be compromised.

It can be noted that in static inclusion we assume that we have a *passive* intruder. A passive intruder is assumed to be able to eavesdrop on message exchanges between agents and use common cryptographic primitives. However, they are not allowed to interact with the principals. A more practical model of an intruder is an active intruder. A problem that is related to static inclusion that allows for an active intruder is known as *observational*

equivalence [2]. Observational equivalence is stronger than both static equivalence and trace equivalence. Due to this, it is often more difficult to check. Thus, more focus has gone into researching static equivalence and trace equivalence.

1.3 Outline

This dissertation is organized as follows. In Chapter 2 we will provide some necessary notation and preliminaries including a formal definition of *static inclusion and equivalence*. We then give some general results on *plats* and *recipes* that will be necessary in later sections, especially the notions of a *pre-cover-set* and a *cover-set*. We provide a definition of $\mathscr{I}$*-closure*, which is a modified version of the one given in [6]. This will enable us to provide some notation and results on $\mathscr{I}$*-independent* substitutions. In Chapter 5 we will provide a method of extending frames which provides a foundation for Chapters 6 and 7. In these chapters we will provide co-saturation procedures for deciding both Δ*-strong intruder theories* and $\omega\triangledown$*-strong intruder theories*. These procedures are the main contributions of this dissertation.

CHAPTER 2
Notation and Preliminaries

We assume the reader is familiar with the usual notions and concepts in term rewriting systems [9] and unification theory [10]. We also recommend that the reader be familiar with the notation and procedures defined in [6].

Let R be a term rewriting system. We say that R is *confluent* if and only if for all terms x, y, and z:

$$y \stackrel{*}{\leftarrow} x \stackrel{*}{\rightarrow} z \Rightarrow y \downarrow z$$

where $\downarrow$ means *joinable*. Recall that two terms x and y are joinable if and only if there is a term z such that $x \stackrel{*}{\rightarrow} z \stackrel{*}{\leftarrow} y$. A term rewriting system R is *terminating* if and only if there does not exist an infinitely descending chain of rewrite steps. If our term rewriting system R is both *confluent* and *terminating*, we say that it is *convergent*. We define R to be *interreduced* if and only if the right hand side r of each rule $l \rightarrow r \in R$ is R-irreducible and the left hand side l is irreducible with respect to $R \setminus \{l \rightarrow r\}$. Let $\succ$ a simplification ordering containing R, i.e., $l \succ r$ for every rule $l \rightarrow r$ in R. A rule $l \succ r$ is *dwindling* if and only if r is a *proper* subterm of l. Given a term t we define $root(t)$ to be the top level symbol of t (i.e., the symbol that occurs at position ε in t). We denote by $\mathscr{P}os(t)$ the set of all positions in t, and by $\mathscr{FP}os(t)$ the set of all non-variable positions in t. By $\mathbf{ST}(t)$ we denote the set of all subterms of t.

A substitution σ is a function that maps variables to terms, i.e., $\sigma : V \mapsto T(F,V)$ such that $\sigma(x) \neq x$ only for finitely many variables, where V is a denumerable set of variables, F is the set of function symbols and $T(F,V)$ is a term algebra. A term t is an *instance* of a term s if and only if there exists a substitution σ such that $\sigma(s) = t$.
We define the domain, range and variable range of a substitution σ as follows:

$$\begin{aligned}
\mathscr{D}om(\sigma) &= \{x \in V \mid \sigma(x) \neq x\}, \\
\mathscr{R}an(\sigma) &= \{\sigma(x) \mid x \in \mathscr{D}om(\sigma)\}, \\
\mathscr{VR}an(\sigma) &= \bigcup_{x \in \mathscr{D}om(\sigma)} \mathscr{V}ar(\sigma(x)).
\end{aligned}$$

Let Names be the set of all constants and $\tilde{n}$ be the set of *private* constants (i.e., the set of nonces). Therefore $\texttt{Names} \setminus \tilde{n}$ is the set of public constants. We assume that Names is infinite.

Definition 1. *A* frame ϕ *is composed of the following:*

1. $\tilde{n}$*,*
2. σ*, a substitution with a finite domain where the* $\mathscr{R}an(\sigma)$ *contains only ground terms.*

Thus $\phi = \nu\tilde{n}.\sigma$*, where* ν *can be considered to be a binding.*

We define our term algebra as follows: $T_\phi = T(F \cup \texttt{Names} \setminus \tilde{n},\ \mathscr{D}om(\sigma))$, where F is our signature and σ is a substitution. Note that F does not contain constants (i.e., function symbols of arity 0) and all elements in F are public. Therefore our function symbols in F are of arity greater than or equal to 1 and F will be interpreted as our cryptographic primitives (i.e., encryption, decryption, etc). Our term algebra T_ϕ is to be interpreted as the intruder's knowledge. We shall refer to the terms in T_ϕ as ϕ-recipes. A term t that is a σ-*instance* of a term in T_ϕ is known as a ϕ-plat.

Now that we have given the necessary notation we will formally define static inclusion and equivalence.

Definition 2. *Given frames* ϕ *and* ψ *and an equational theory* $\approx$*, we say that* ϕ *is statically included in* ψ *under* $\approx$*, and write* $\phi \sqsubseteq_S \psi$*, if* $T_\phi = T_\psi$ *(i.e.,* $\mathscr{D}om(\sigma) = \mathscr{D}om(\rho)$*) and* $\forall t,t' \in T_\phi$*, if* $\sigma(t) \approx \sigma(t')$ *then* $\rho(t) \approx \rho(t')$*.*

Note that static equivalence is simply static inclusion in both directions.

Definition 3. *Given frames* ϕ *and* ψ *and an equational theory* $\approx$*, we say that* ϕ *and* ψ *are statically equivalent under* $\approx$*, and write* $\phi \approx_S \psi$*, if* $T_\phi = T_\psi$ *(i.e.,* $\mathscr{D}om(\sigma) = \mathscr{D}om(\rho)$*) and* $\forall t,t' \in T_\phi, \sigma(t) \approx \sigma(t')$ *if and only if* $\rho(t) \approx \rho(t')$*.*

Let R be a convergent term rewriting system. An n-ary public symbol f is said to be *transparent for* R, or R*-transparent*, if and only if there exist cap-terms $C_1^f(\diamond), \ldots, C_n^f(\diamond)$ such that $C_i^f[f(x_1,\ldots,x_n)] \rightarrow_R^* x_i$, for every $1 \leq i \leq n$ where $x_1, \ldots x_n$ are distinct variables.

Note that we use the definition of a cap term as given in [6]. We will denote the hole variable in $C_i^f(\diamond)$ being "filled" with a term t as $C_i^f[t]$. A public function symbol is *R-resistant* if and only if it is not R-transparent. Note that R may be omitted if the term rewriting system is clear from the context.

Throughout this dissertation we shall assume that our term rewriting systems are convergent and interreduced, and frame substitutions (i.e., σ and ρ) are normalized substitutions.

CHAPTER 3
General results on frames, recipes, and plats

Throughout this chapter we assume that $\phi = \nu\tilde{n}\,.\,\sigma$ is a frame and that V is a denumerable set of variables disjoint from $\mathscr{D}om(\sigma)$. Furthermore, for ease of exposition, we separate public names, i.e., those in $(\mathtt{Names} \setminus \tilde{n})$, into two sets: names that already appear in $\mathscr{R}an(\sigma)$ which we call n_{frame}, and names that are "brand new", n_{new}. Thus $\mathtt{Names}$ can be partitioned into the following three sets: $\tilde{n} \uplus n_{\text{frame}} \uplus n_{\text{new}}$. This notation will help provide more clarity in some of the following proofs in this chapter.

Definition 4. *A term t that is a σ-instance of a term in T_ϕ is known as a ϕ-plat or simply a plat if the frame is clear from the context. We shall denote the set of all ϕ-plats as Π_ϕ.*

Recall that terms in T_ϕ are known as ϕ-recipes. Note that we chose the name plat since in French plat means meal. Thus, intuitively, we are building our ϕ-plats or "meals" from ϕ-recipes.

Now we will define a more general variant of a ϕ-recipe that we shall denote as a *general recipe* which intuitively is a recipe with the addition of variables.

Definition 5. *A term $t \in T(F \cup \mathtt{Names} \setminus \tilde{n},\, V \cup \mathscr{D}om(\sigma))$ is said to be a general recipe.*

In other words, a term t is a general recipe if and only if one of the following holds:

1. $t \in V$.
2. $t \in (\mathtt{Names} \setminus \tilde{n})$.
3. $t \in \mathscr{D}om(\sigma)$.
4. $t = f(t_1, \ldots, t_n)$ where every t_i, $1 \leq i \leq n$, is a general recipe.

A concept that we will use heavily is that of a generalized form of a plat which we will denote as a *general plat*. We will start by defining a general plat and then we will provide several alternative yet equivalent characterizations of general plats that will sometimes be used implicitly in proofs throughout this dissertation.

Definition 6. *A term $t \in T(F \cup \mathtt{Names}, V)$ is said to be a general plat if and only if $\theta(t)$ is a plat for all substitutions $\theta : \mathscr{V}ar(t) \longmapsto (\mathtt{Names} \setminus \tilde{n})$.*

We are now ready to give several alternative characterizations of general plats.

Lemma 3.0.1. *A term $s \in T(F \cup \mathtt{Names}, V)$ is a general plat if and only if there exists a substitution $\beta : \mathscr{V}ar(s) \longmapsto n_{new}$ such that $\beta(s)$ is a plat.*

Proof. The "only if" part follows from the definition of general plats. To prove the "if" part let $\theta : \mathscr{V}ar(s) \longmapsto n_{new}$ be a substitution. We prove that if $\theta(s)$ is a plat, then so is $\theta'(s)$ for all substitutions $\theta' : \mathscr{V}ar(s) \longmapsto (\mathtt{Names} \setminus \tilde{n})$. We prove this by contradiction. Let s be a minimal counterexample in terms of size, i.e., there are substitutions $\theta : \mathscr{V}ar(s) \longmapsto n_{\text{new}}$ and $\theta' : \mathscr{V}ar(s) \longmapsto (\mathtt{Names} \setminus \tilde{n})$ such that $\theta(s)$ is a plat whereas $\theta'(s)$ is not. Note that $\theta(s)$ cannot be a term from $\mathscr{R}an(\sigma)$ since there are new names in it. Thus s must be of the form $f(s_1, \ldots, s_n)$ such that $\theta(s_i)$ is a plat for $1 \leq i \leq n$. Since s is assumed to be a minimal counterexample, $\theta'(s_i)$ must also be a plat for $1 \leq i \leq n$. But then $\theta'(s)$ will also be a plat. □

The following alternative characterization will be used in many of our proofs. Note that this characterization is a recursive definition of a general plat. It is defined in a similar style as a term in term rewriting.

Lemma 3.0.2. *A term $t \in T(F \cup \mathtt{Names}, V)$ is a general plat if and only if one of the following holds:*

1. *$t \in V$.*
2. *$t \in (\mathtt{Names} \setminus \tilde{n})$.*
3. *$t \in \mathscr{R}an(\sigma)$.*
4. *$t = f(t_1, \ldots, t_n)$ where every t_i, $1 \leq i \leq n$, is a general plat.*

Proof. The "if" part is straightforward. We prove the "only if" part by contradiction. Let s be a minimal counterexample in terms of size, i.e., s is a general plat, where s is neither a variable nor a public constant, $s \notin \mathscr{R}an(\sigma)$ and s is not of the form $f(s_1, \ldots, s_n)$ where every top-level subterm is a general plat. Since s is neither a variable nor a constant, s

has to be of the form $f(s_1,\ldots,s_n)$ such that at least one top-level subterm, say s_k, is not a general plat. Hence s cannot be a ground term (i.e., a plat) either. Let $\eta : \mathscr{V}ar(s) \longmapsto (\texttt{Names} \setminus \tilde{n})$ be a substitution that replaces every variable in s with a *new constant*. Since $\eta(s)$ is a plat, there must be a recipe s' such that $\eta(s) = \sigma(s')$. Since s is non-ground, $\eta(s)$ cannot be a term from $\mathscr{R}an(\sigma)$ and thus $s' \notin \mathscr{D}om(\sigma)$. Thus s' has to be of the form $f(s'_1,\ldots,s'_n)$ where each top-level subterm of s' is a recipe as well. Therefore $\eta(s_k) = \sigma(s'_k)$. Thus $\eta(s_k)$ is a plat, and by Lemma 3.0.1 we get a contradiction. □

Lemma 3.0.3. *A term $t \in T(F \cup \texttt{Names}, V)$ is a general plat if and only if there is a general recipe s such that $t = \sigma(s)$.*

Proof. We only prove the "only if" part because the "if" part will use a similar argument. This proof is by structural induction on the term tree representation of t. By Definition 5 and Lemma 3.0.2 we know that general recipes and plats must both be in one of four forms. We will only consider non-ground terms since a ground general plat (resp., recipe) is a plat (resp., recipe). Our base case occurs when our term tree has only one node, which means that t must be a variable and thus a general recipe.

The fourth case for general plats will be our inductive case. If $t_1,\ldots,t_n$ are general plats and have corresponding general recipes $s_1,\ldots,s_n$ then $f(t_1,\ldots,t_n)$ is also a general plat with the general recipe $f(s_1,\ldots,s_n)$. □

Lemma 3.0.4. *Let $s = f(s_1,\ldots,s_n)$ be a plat. If at least one of the s_i's is not a plat, then $s \in \mathscr{R}an(\sigma)$.*

Proof by contradiction. We shall assume that at least one of the s_i's is not a plat and $s \notin \mathscr{R}an(\sigma)$. Since s is a plat we can write it as $\sigma(t) = s$ for some term $t \in T_\phi$. This recipe t can be either a variable or of the form $f(t_1,\ldots,t_n)$, where the t_i's are recipes. If t is a variable then $t \in \mathscr{D}om(\sigma)$ and thus $\sigma(t) = s$ is in $\mathscr{R}an(\sigma)$, which is a contradiction. Otherwise $s = f(s_1,\ldots,s_n) = \sigma(f(t_1,\ldots,t_n))$ which means that $\sigma(t_1) = s_1,\ldots,\sigma(t_n) = s_n$. However this is a contradiction since the t_i's are recipes and thus the s_i's are plats. □

Corollary 3.0.5. *Let s be a plat and $p \in \mathscr{P}os(s)$ such that $s|_p$ is not a plat. Then there exists a position $\varepsilon \preceq q \prec p$ such that $s|_q \in \mathscr{R}an(\sigma)$.*

Proof. We prove this by contradiction. Let s be a minimal counterexample with respect to term size, i.e., s is a ϕ-plat, $p \in \mathscr{P}os(s)$ such that $s|_p$ is not a ϕ-plat, and $s|_q \notin \mathscr{R}an(\sigma)$

for all $\varepsilon \preceq q \prec p$. Clearly s must be of the form $f(s_1,\ldots,s_n)$ and $p = i\cdot\hat{p}$ where $1 \leq i \leq n$. If s_i itself is not a ϕ-plat then we have a contradiction by Lemma 3.0.4. Else s_i is a ϕ-plat and a subterm of s_i, namely $s_i|_{\hat{p}}$ is not a ϕ-plat. However, this contradicts the minimality of s since s_i will be a smaller counterexample. □

Lemma 3.0.6. *A term $t \in T(F \cup \mathtt{Names}, V)$ is a general plat if and only if $\theta(t)$ is a plat for all substitutions $\theta : \mathscr{V}ar(t) \longmapsto \Pi_\phi$.*

Proof. We first prove the following claim:

> **Claim**: Let $s \in T(F \cup \mathtt{Names}, V)$ be a term and $\theta : \mathscr{V}ar(s) \longmapsto n_{new}$ be a substitution. If $\theta(s)$ is a plat, then so is $\theta'(s)$ for all substitutions $\theta' : \mathscr{V}ar(s) \longmapsto \Pi_\phi$.
>
> **Proof**: The proof is again by contradiction. Let s be a minimal counterexample to this in terms of size, i.e., there are substitutions $\theta : \mathscr{V}ar(s) \longmapsto n_{\text{new}}$ and $\theta' : \mathscr{V}ar(s) \longmapsto \Pi_\phi$ such that $\theta(s)$ is a plat whereas $\theta'(s)$ is not. Note that $\theta(s)$ cannot be a term from $\mathscr{R}an(\sigma)$ since there are new names in it. Thus s must be of the form $f(s_1,\ldots,s_n)$ such that $\theta(s_i)$ is a plat for $1 \leq i \leq n$. Since s is assumed to be a minimal counterexample, $\theta'(s_i)$ must also be a plat for $1 \leq i \leq n$. But then $\theta'(s)$ will also be a plat. □

The remainder of this proof is shown by Lemma 3.0.1. □

Lemma 3.0.7. *Let $t \in T(F \cup \mathtt{Names}, V)$ and let $\theta : \mathscr{V}ar(t) \longmapsto T(F \cup \mathtt{Names})$ be a substitution. If t is not a general ϕ-plat and $\theta(t)$ is a ϕ-plat, then there exists a position $p \in \mathscr{FP}os(t)$ such that $t|_p$ is a non-ground term and $\theta(t|_p) \in \mathscr{R}an(\sigma)$.*

Proof. We prove this by contradiction. Let t be a minimal counterexample with respect to term size, i.e., t is not a general plat, $\theta(t)$ is a plat and $\theta(t|_p) \notin \mathscr{R}an(\sigma)$ for all $p \in \mathscr{FP}os(t)$. Thus t cannot be a variable or a ground term. It cannot be that $\theta(t) \in \mathscr{R}an(\sigma)$ for if so, then $p = \varepsilon$ and we have a contradiction. Thus t must be of the form $f(t_1,\ldots,t_n)$ where $\theta(t_i)$ is a ϕ-plat for all $1 \leq i \leq n$. (Since $\theta(f(t_1,...,t_n)) \notin \mathscr{R}an(\sigma)$ all top level subterms of f must be plats.) We know that some t_j, where $1 \leq j \leq n$, must not be a

general plat since t is not a general plat. However, this contradicts the minimality of t since t_i will be a smaller counterexample. □

Note that the converse of Lemma 3.0.7 is not true. Consider the frame $\nu\{b\}.\sigma$ where $\sigma = \{x \mapsto f(a,b)\}$. Let $t = f(a,y)$ and $\theta = \{y \mapsto b\}$. Now t is a general plat, but $\theta(t|_\varepsilon) \in \mathscr{R}an(\sigma)$.

Lemma 3.0.8. *Let $t \in T(F \cup \mathtt{Names}, V)$ and let $\theta : \mathscr{V}ar(t) \longmapsto T(F \cup \mathtt{Names})$ be a substitution such that $\theta(t)$ is a ϕ-plat. If $\theta(t|_p) \notin \mathscr{R}an(\sigma)$ for all positions $p \in \mathscr{FP}os(t)$, then t is a general plat and $\theta(x) \in \Pi_\phi$ for all $x \in \mathscr{V}ar(t)$ (i.e., $\theta : \mathscr{V}ar(t) \longmapsto \Pi_\phi$).*

Proof. Follows from Corollary 3.0.5 and Lemma 3.0.7.

□

Definition 7. *A substitution $\widehat{\sigma}$ is a plat-extension of σ if and only if*

1. $\sigma \subseteq \widehat{\sigma}$ *and*
2. $\forall x \in (\mathscr{D}om(\widehat{\sigma}) \setminus \mathscr{D}om(\sigma)) : \widehat{\sigma}(x)$ is a ϕ-plat.

The following two notions that we will define, *pre-cover-set* and *cover-set*, will be crucial concepts in understanding the co-saturation procedures that we will provide in Chapters 6 and 7.

Lemma 3.0.9. *For any term $t \in T(F \cup \mathtt{Names}, V)$ there exists a finite set S of general plats such that*

(1) every term $s \in S$ is an instance of t.

(2) for all substitutions $\theta : \mathscr{V}ar(t) \longmapsto T(F \cup \mathtt{Names})$, if $\theta(t)$ is a plat, then there exists a general plat $s \in S$ and a substitution $\eta : \mathscr{V}ar(t) \longmapsto \Pi_\phi$ such that $\theta(t) = \eta(s)$.

(We refer to these sets by the phrase "pre-cover sets".)

Proof. We first outline the construction of the pre-cover set S for t:

If t itself is a general plat, then $t \in S$. Now for all positions p in $\mathscr{FP}os(t)$ such that $t|_p$ is a *non-ground term* which can be matched with a term in $\mathscr{R}an(\sigma)$, we define

$$\beta_p^j \;=\; mgu(t|_p \lesssim^? \sigma(X_j))$$

where $X_j \in \mathscr{D}om(\sigma)$ and $t|_p$ matches with $\sigma(X_j)$. Now we can define the pre-cover-set recursively as follows:

$$S = \begin{cases} \{t\} \cup \bigcup\limits_{p \in \mathscr{FP}os(t)} \text{pre-cover-set}(\beta_p^j(t)) & \text{if } t \text{ is a general plat} \\ \\ \bigcup\limits_{p \in \mathscr{FP}os(t)} \text{pre-cover-set}(\beta_p^j(t)) & \text{otherwise.} \end{cases} \tag{3.1}$$

This procedure is clearly terminating since the number of variables is decreasing with each recursive call: note that we are only matching non-ground subterms with terms in $\mathscr{R}an(\sigma)$.

To prove (2) we will consider the following two main cases. Let θ be any substitution such that $\theta(t)$ is a ϕ-plat.

(a) There does not exist a position $p \in \mathscr{FP}os(t)$ such that $t|_p$ is non-ground and can be matched with a term in $\mathscr{R}an(\sigma)$: this case is handled by Lemma 3.0.8.

(b) There exists a position $p \in \mathscr{FP}os(t)$ such that $t|_p$ is non-ground and can be matched with a term in $\mathscr{R}an(\sigma)$. Thus $t|_p$ must contain at least one variable.

Since we compute the pre-cover set recursively on $t|_p$, we can show that the result of all the recursive calls is as follows:

$$\theta = \widehat{\theta} \circ \beta_{p_n}^{j_m} \circ \cdots \circ \beta_{p_1}^{j_1}$$

where $p_1, \ldots, p_n$ are positions in $\mathscr{FP}os(t)$, $X_{j_1}, \ldots X_{j_m}$ are terms in $\mathscr{D}om(\sigma)$ such that $t|_{p_k}$ is matchable to $\sigma(X_{j_k})$ with $1 \leq k \leq n$ and $1 \leq j \leq m$. By our initial assumption in this case we know that at least one such β_p^j must exist.

Since θ and the β_p^j are all ground substitutions we can say:

$$\widehat{\theta} = \theta \setminus \left\{ \beta_{p_n}^{j_m} \circ \cdots \circ \beta_{p_1}^{j_1} \right\}$$

Note that the β_p^j's can only replace the variables in t that can match with a proper subterm of a term in $\mathscr{R}an(\sigma)$, the remaining variables in t have to be replaced with ϕ-plats. Thus what is left after all the β_p^j's are applied is a substitution $\widehat{\theta}$ that will map the variables in t to ϕ-plats. Thus, η is equal to $\widehat{\theta}$.

Now we must show that there exists an s such that $\theta(t) = \eta(s)$. This is obvious since we can choose our s to be $\beta_{p_n}^{j_m} \circ \cdots \circ \beta_{p_1}^{j_1}(t)$. Thus, $\theta(t) = \widehat{\theta}\left(\beta_{p_n}^{j_m} \circ \cdots \circ \beta_{p_1}^{j_1}(t)\right) = \eta\left(\beta_{p_n}^{j_m} \circ \cdots \circ \beta_{p_1}^{j_1}(t)\right)$.

□

Examples: Let $\nu\{a\}.\sigma$ be a frame where $\sigma = \left\{X_1 \mapsto f(g(a),a),\ X_2 \mapsto g(g(a))\right\}$.

(i) Let $t = f(g(u),a)$, then $\mathscr{FP}os(t) = \{\varepsilon, 1, 2\}$. Note that t itself is not a general plat, but $t|_\varepsilon = t$ can be matched with $\sigma(X_1)$ and $t|_1 = g(u)$ can be matched with $\sigma(X_2)$. Thus $\beta_\varepsilon^1 = \{u \mapsto a\}$ and $\beta_1^2 = \{u \mapsto g(a)\}$. Now $\beta_\varepsilon^1(t) = f(g(a),a)$ which is a ground plat, whereas $\beta_1^2(t) = f(g(g(a)),a)$ which, though ground, is not a plat. Thus pre-cover-set$(t) = \{f(g(a),a)\}$.

(ii) Let $t = f(g(u),v)$, then $\mathscr{FP}os(t) = \{\varepsilon, 1\}$. Note that t is a general plat, and besides $t|_\varepsilon = t$ can be matched with $\sigma(X_1)$ and $t|_1 = g(u)$ can be matched with $\sigma(X_2)$. Thus $\beta_\varepsilon^1 = \{u \mapsto a,\ v \mapsto a\}$ and $\beta_1^2 = \{u \mapsto g(a)\}$. Now $\beta_\varepsilon^1(t) = f(g(a),a)$ is a ground plat (as in Case (i) above) and $\beta_1^2(t) = f(g(g(a)),v)$ which is a general plat. Therefore pre-cover-set$\left(\beta_\varepsilon^1(t)\right) = \{f(g(a),a)\}$ and the pre-cover-set$\left(\beta_1^2(t)\right)$ turns out to be $\{f(g(g(a)),v)\}$ since there is no non-variable non-ground subterm of $f(g(g(a)),v)$ which matches with a term in the range of σ. □

Lemma 3.0.10. *For any term $t \in T(F \cup \mathtt{Names},\ V)$ that has an instance which is a ϕ-plat, there exists a finite set S of general recipes such that*

1. *for all terms* $s \in S$: $\sigma(s)$ *is an instance of* t, *and*

2. *for all substitutions* $\theta : \mathcal{V}ar(t) \longmapsto T(F \cup \mathtt{Names})$, *if* $\theta(t)$ *is a* ϕ*-plat, then there exists a general recipe* $\tau \in S$ *and a plat-extension* $\widehat{\sigma}$ *of* σ *such that* $\theta(t) = \widehat{\sigma}(\tau)$.

This set is referred to as a cover-set for t *with respect to* ϕ.

Proof. By Lemma 3.0.9, we only need to show that for every general plat there is a general recipe. Thus by Lemma 3.0.3 we are done. □

Example 3.0.11. *Let* $\phi = \nu\{a,b\}\,.\,\{X_1 \mapsto g_1(a),\ X_2 \mapsto f(g_1(a),b)\}$ *be a frame and* $t = f(g_1(u),v)$ *be a term. The cover-set is* $\{f(g_1(u),v),\ f(X_1,v),\ X_2\}$.
Note that $\{f(g_1(u),v)\}$ *is not a cover-set by itself, since there is no plat-extension that maps* $f(g_1(u),v)$ *to* $f(g_1(a),b)$.

For additional examples please see Appendix B.

We also consider cover-sets of *equations* — this essentially amounts to considering equality (=) as a binary function symbol. Additionally we can consider the *cover-set of a convergent term rewriting system R*. As R is a set of rewrite rules $l \to r$, we can consider each rule as an equation of the form $l =_R r$. Now to compute the cover-set of R we simply take the union of the cover-sets of all such equations. It is worth noting here that for such rules the equation $l =_R r$ itself will be in the cover-set, since it contains no hidden nonces.

Example 3.0.12. *Let* $\phi = \nu\{a,b\}\,.\,\{X_1 \mapsto g(a),\ X_2 \mapsto h(h(b))\}$ *be a frame and* $f(g(x),h(y)) = g(x)$ *be an equation denoted by eq. The cover-set for eq with respect to* ϕ *is as follows:*

$$\Big\{f(g(x),h(y)) = g(x),\ \ f(X_1,h(y)) = X_1,\ \ f(g(x),X_2) = g(x),\ \ f(X_1,X_2) = X_1\Big\}$$

The size of a cover-set can be exponential. This will be illustrated in the following example:

Example 3.0.13. *Let* $\phi = \nu\{a,b\}.\{X_1 \mapsto g(a), X_2 \mapsto g(b)\}$ *be a frame and* $t = f(g(u_1), f(g(u_2), ..., g(u_n)))$ *be a term. The cover-set for* t *with respect to* ϕ *will*

contain all recipe terms of the form:

$$f(X_{i_1}, f(X_{i_2}, ..., X_{i_n}))$$

where $i_j \in \{1,2\}$ for all j. For a term tree representation of this term, please see figure 3. Note that the variables $u_1, ..., u_n$ can all be replaced by either a or b, thus we have 2^n possibilities.

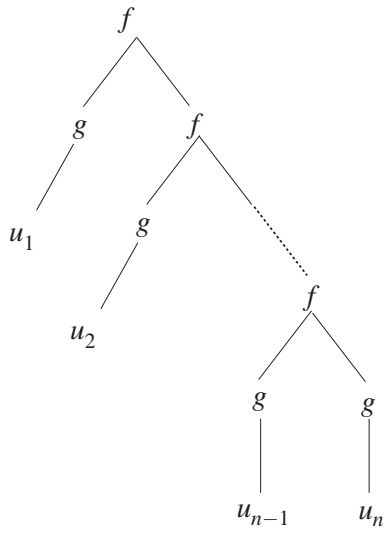

Figure 3.1: Term tree representation

Definition 8. *Let R be a convergent term rewriting system and let $\phi = \nu\tilde{n}.\sigma$ and $\psi = \nu\tilde{n}.\rho$ be frames. A mapping $(x_i \mapsto s_i)$ in σ is syntactically redundant with respect to ρ if and only if there exists a recipe $r \in T(F \cup \mathtt{Names} \setminus \tilde{n},\ \mathscr{D}om(\sigma) \setminus \{x_i\})$ such that $s_i = \sigma(r)$ and $\rho(x_i) =_R \rho(r)$.*

Example 3.0.14. *Let $R = \{d(e(x,y),y) \to x,\ e(d(x,y),y) \to x\}$ and let*

$$\phi = \nu\tilde{n}.\sigma = \nu\{a,k,k_1\}.\{X_1 \mapsto e(a,k),\ X_2 \mapsto k,\ X_3 \mapsto a\}$$

and

$$\psi = \nu\tilde{n}.\rho = \nu\{a,k,k_1\}.\{X_1 \mapsto e(a,k),\ X_2 \mapsto k_1,\ X_3 \mapsto d(e(a,k),k_1)\}$$

be frames. The mapping $X_1 \mapsto e(a,k)$ is syntactically redundant with respect to ρ, since

$$X_1 = \sigma(e(X_3, X_2))$$

and

$$\rho(e(X_3, X_2) = e(d(e(a,k),k_1),k_1) \rightarrow_R^! e(a,k) = \rho(X_1).$$

CHAPTER 4
General results on $\mathscr{I}$-*independent* substitutions

Now we will provide a modified definition of $\mathscr{I}$-closure. We will use the notions of $\mathscr{I}$-closure, $\mathscr{I}$-independence and $\mathscr{I}$-cores when we are performing checks after running our procedures. Intuitively they are used to identify non-redundant information.

Definition 9. *Let S be a finite set such that $S \subseteq \tilde{n}$. We define the $\mathscr{I}$-closure of S, denoted by $\mathscr{I}(S)$, as follows:*

- $S \subseteq \mathscr{I}(S)$
- *If $f^{(p)}$ is a function symbol and $s_1, \ldots s_p$ are in $\mathscr{I}(S)$, then* $f(s_1, \ldots s_p) \in \mathscr{I}(S)$
- *Nothing else is in $\mathscr{I}(S)$.*

In other words, a term $t \in \tilde{n}$ is in $\mathscr{I}(S)$ if and only if either t itself is in S, or the root symbol of $t \in F$ and all its top-level subterms are in $\mathscr{I}(S)$.

Definition 10. *A set of terms $\Gamma = \{t_1, \ldots, t_n\}$ is $\mathscr{I}$-independent if and only if for all t_i, we have $t_i \notin \mathscr{I}(\Gamma \setminus \{t_i\})$. A ground substitution θ is $\mathscr{I}$-independent if and only if $\mathscr{R}an(\theta)$ is an $\mathscr{I}$-independent set and $\forall v_i, v_j \in \mathscr{D}om(\theta) : \theta(v_i) = \theta(v_j) \Leftrightarrow v_i = v_j$. A ground substitution θ is $\mathscr{I}$-dependent if and only if it is not $\mathscr{I}$-independent.*

Lemma 4.0.15. *If σ syntactically unifies two distinct recipes then σ must be $\mathscr{I}$-dependent.*

Proof. We will prove this by contradiction. We will assume that σ syntactically unifies two distinct recipes r_1 and r_2 and, besides, σ is $\mathscr{I}$-independent. Let (r_1, r_2) be a minimal counterexample in terms of $|r_1| + |r_2|$. Neither r_1 nor r_2 can be a variable, since that would contradict the $\mathscr{I}$-independence of σ. We know that r_1 and r_2 are both of the form $f(t_1, \ldots, t_n)$ since we know that they are both syntactically unifiable their root symbols and arities must be the same. However, r_1 and r_2 are assumed to be distinct recipes so they must differ at a subterm, so without loss of generality we can say that they differ at position $p \in \mathscr{P}os(r_1)$ and $\mathscr{P}os(r_2)$ where $p \neq \varepsilon$. However, this contradicts minimality

since $s_1 = r_1|_p$ and $s_2 = r_2|_p$ are two distinct recipes that are unified by σ and $|s_1| + |s_2| < |r_1| + |r_2|$. □

Lemma 4.0.16. *Let σ be an $\mathscr{I}$-independent substitution, τ_r a recipe, and l be any term. If $\sigma(\tau_r)$ is an instance of l and $Pos(l) \subseteq Pos(\tau_r)$, then τ_r is an instance of l.*

Proof. We will prove this by contradiction. The case where l is linear is trivial. If l is non-linear and l does not match τ_r, then there must be a variable $y \in \mathscr{V}ar(l)$ and distinct positions $p, q \in \mathscr{P}os(l)$ such that $y = l|_p = l|_q$ and $\tau_r|_p \neq \tau_r|_q$. Since σ is an $\mathscr{I}$-independent substitution, we know by Lemma 4.0.15 that σ cannot syntactically unify two distinct recipes. Thus this is a contradiction. □

Definition 11. *A set S_1 of terms is an $\mathscr{I}$-core of a set of terms S_2 if and only if $S_1 \subseteq S_2$, S_1 is $\mathscr{I}$-independent and every term in $S_2 \setminus S_1$ belongs to $\mathscr{I}(S_1)$.*

Now that we have the notion of $\mathscr{I}$-independence we can define the set of all non-redundant mappings of a substitution θ, which we will denote as *$\mathscr{I}$-core(θ)*:

Definition 12. *A substitution θ_1 is an $\mathscr{I}$-core of a substitution θ_2 if and only if $\theta_1 \subseteq \theta_2$, θ_1 is $\mathscr{I}$-independent and $\mathscr{R}an(\theta_1)$ is an $\mathscr{I}$-core of $\mathscr{R}an(\theta_2)$.*

CHAPTER 5
Static Inclusion

Throughout this chapter and remaining chapters we shall assume that $\phi = \nu\tilde{n}.\sigma$, $\phi' = \nu\tilde{n}.\sigma'$, $\psi = \nu\tilde{n}.\rho$, and $\psi' = \nu\tilde{n}.\rho'$ are frames. In this chapter we shall give a formal definition of static inclusion and the basic framework for how we will be able to extend frames. We are able to model an intruder's growing knowledge by extending these frames.

Recall the following definitions of static inclusion and static equivalence, given in Chapter 2.

Definition 13. *Given frames ϕ and ψ and an equational theory $\approx$, we say that ϕ is statically included in ψ under $\approx$, and write $\phi \sqsubseteq_S \psi$, if $T_\phi = T_\psi$ (i.e., $\mathscr{D}om(\sigma) = \mathscr{D}om(\rho)$) and $\forall t, t' \in T_\phi$, if $\sigma(t) \approx \sigma(t')$ then $\rho(t) \approx \rho(t')$.*

Definition 14. *Given frames ϕ and ψ and an equational theory $\approx$, we say that ϕ and ψ are statically equivalent under $\approx$, and write $\phi \approx_S \psi$, if $T_\phi = T_\psi$ (i.e., $\mathscr{D}om(\sigma) = \mathscr{D}om(\rho)$) and $\forall t, t' \in T_\phi, \sigma(t) \approx \sigma(t')$ if and only if $\rho(t) \approx \rho(t')$.*

We shall now discuss the notion of a simple extension. This definition will be a key part of our co-saturation procedure, since they will be used to extend our frames' substitutions. Extending these substitutions is how we will model the intruders knowledge over the course of the protocol's runtime. Recall Example 1.1.1, where we extended ρ to model the intruder guessing a key k'.

Definition 15. *A frame ϕ' is called a simple extension of ϕ if and only if $\sigma \subset \sigma'$ and $|\sigma'| = |\sigma| + 1$. In other words, σ and σ' are of the form*

$$\sigma = \{x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n\}$$

and,

$$\sigma' \;=\; \sigma \uplus \{x_{n+1} \mapsto t_{n+1}\}.$$

Lemma 5.0.17. *Let R be a convergent term rewriting system and let ϕ, ϕ', ψ, and ψ' be frames such that*

(a) $\mathscr{D}om(\sigma) = \mathscr{D}om(\rho)$, $\mathscr{D}om(\sigma') = \mathscr{D}om(\rho')$ *and*

(b) ϕ' *is a simple extension of* ϕ *and* ψ' *is a simple extension of* ψ.

If $\phi' \sqsubseteq_S \psi'$ *then* $\phi \sqsubseteq_S \psi$.

Proof by contradiction. Assume that $\phi' \sqsubseteq_S \psi'$ and $\phi \not\sqsubseteq_S \psi$. Since ϕ' is a simple extension of ϕ (respectively for ψ' and ψ), we know that $\sigma' = \sigma \uplus \{x_{n+1} \mapsto t_{n+1}\}$ and $\rho' = \rho \uplus \{x_{n+1} \mapsto s_{n+1}\}$ for some ground terms $s_{n+1},\ t_{n+1}$ where $n = |\sigma| = |\rho|$. Thus we have

$$\nu\tilde{n}.\{\sigma \uplus \{x_{n+1} \mapsto t_{n+1}\}\} \sqsubseteq_S \nu\tilde{n}.\{\rho \uplus \{x_{n+1} \mapsto s_{n+1}\}\} \text{ and } \nu\tilde{n}.\sigma \not\sqsubseteq_S \nu\tilde{n}.\rho.$$

Therefore for some $t, t' \in T_\phi, \sigma(t) \downarrow_R \sigma(t')$ but $\rho(t) \not\downarrow_R \rho(t')$. By definition we have that $T_\phi \subseteq T_{\phi'}$; thus t, t' must also be $\in T_{\phi'}$, and besides, $\sigma'(s) = \sigma(s)$ and $\rho'(s) = \rho(s)$ for all $s \in T_\phi$. Since $\phi' \sqsubseteq_S \psi'$ we know that if $\sigma'(t) \downarrow_R \sigma'(t')$ then $\rho'(t) \downarrow_R \rho'(t')$, which is a contradiction. □

Lemma 5.0.18. *Let R be a convergent term rewriting system and let* ϕ, ϕ', ψ, *and* ψ' *be frames such that*

(a) $\mathscr{D}om(\sigma) = \mathscr{D}om(\rho)$, $\mathscr{D}om(\sigma') = \mathscr{D}om(\rho')$ *and*

(b) ϕ' *is a simple extension of* ϕ *(respectively for* ψ' *and* ψ*)*

Let $\{x_{n+1} \mapsto s_{n+1}\} = \sigma' \setminus \sigma$ *and* $\{x_{n+1} \mapsto t_{n+1}\} = \rho' \setminus \rho$.*If there exists a recipe* $r \in T_\phi$ *such that* $s_{n+1} =_R \sigma(r)$ and $t_{n+1} =_R \rho(r)$ *then* ($\phi \sqsubseteq_S \psi$ *if and only if* $\phi' \sqsubseteq_S \psi'$).

Proof (only-if) by contradiction. Assume $\phi \sqsubseteq_S \psi$ and $\phi' \not\sqsubseteq_S \psi'$, i.e., there are ϕ'-recipes τ_1 and τ_2 such that $\sigma'(\tau_1) \downarrow_R \sigma'(\tau_2)$ and $\rho'(\tau_1) \not\downarrow_R \rho'(\tau_2)$. However, we know that there exists an $r \in T_\phi$ such that $s_{n+1} =_R \sigma(r)$ and $t_{n+1} =_R \rho(r)$. For every ϕ'-recipe s, let $s^\phi = \{x_{n+1} \mapsto r\}(s)$. Thus $\sigma'(s) = \sigma(s^\phi)$ and $\rho'(s) = \rho(s^\phi)$ since $s_{n+1} =_R \sigma(r)$ and $t_{n+1} =_R \rho(r)$. This leads to $\sigma(\tau_1^\phi) \downarrow_R \sigma(\tau_2^\phi)$ and $\rho(\tau_1^\phi) \not\downarrow_R \rho(\tau_2^\phi)$ which contradicts $\phi \sqsubseteq_S \psi$. □

Proof (if). This proof is straightforward since it is a special case of Lemma 5.0.17. □

CHAPTER 6
Δ-strong Intruder Theories

In this chapter we will be defining Δ-strong intruder theories and then we will provide our co-saturation procedure for these theories. We will assume that our intruder theory is Δ-strong and recall that it is also convergent and Interreduced. There are many Δ-strong intruder theories that are useful in practice. Some of these theories are Homomorphic Encryption [5], Blind Signatures [6], and a 2-sorted Equational theory for Cipher-Decipher Block Chaining [4].

We shall now introduce a co-saturation procedure that was inspired by "Intruders with Caps." We refer to our co-saturation method as a procedure since it solves the static inclusion decision problem. However, our procedure is an algorithm as we will show soundness, completeness, and termination for Δ-strong intruder theories.

Definition 16. *Let R be any convergent intruder term rewriting system, and $\succ$ a simplification ordering on R. We assume that $\succ$ is a precedence based ordering that satisfies the block-ordering property: every private symbol is higher than every public symbol under $\succ$.*

Definition 17. *Let R be any convergent intruder term rewriting system, and $\succ$ a simplification ordering on R. A rewrite rule $l \to r$ is said to be Δ-strong, with respect to the simplification ordering $\succ$, if and only if every R-resistant subterm of l is greater than r with respect to $\succ$. The intruder term rewriting system R is said to be Δ-strong with respect to $\succ$ if and only if every rule is Δ-strong with respect to $\succ$.*

Note that a definition of Δ-strong appeared in "Intruders with Caps" [6]. Our definition differs from theirs since we only allow Δ-strong rules. In [6] they defined Δ-strong theories to contain either Δ-strong rules or dwindling rules. Also, we only consider function symbols to be public, since in practice cryptographic primitives are generally known to all agents including intruders. For example in the RSA cryptosystem [24, 32] both the encryption and decryption operations (namely, modular exponentiation) are made publicly available. In [6] function symbols could be public or private.

Definition 18. *Let R be a convergent term rewriting system, σ a ground substitution and S a set of terms over $T(F \cup \mathtt{Names}, \mathscr{D}om(\sigma))$. Then by $(\sigma(S))\downarrow_R$ we denote a set of normal forms of terms in S instantiated by σ.*

Definition 19. *Let $\phi = \nu\tilde{n}.\sigma$ be a frame, $t \in \mathscr{R}an(\sigma)$ such that the root symbol of t is R-resistant, $l \to r$ a rule in R and $\theta = mgu(l|_p =^? t)$ where $p \in \mathscr{FP}os(l)$. If $\theta(l)$ has an instance which is a plat, then $\theta(l)$ is said to be the s-overlap of l and t at position p.*

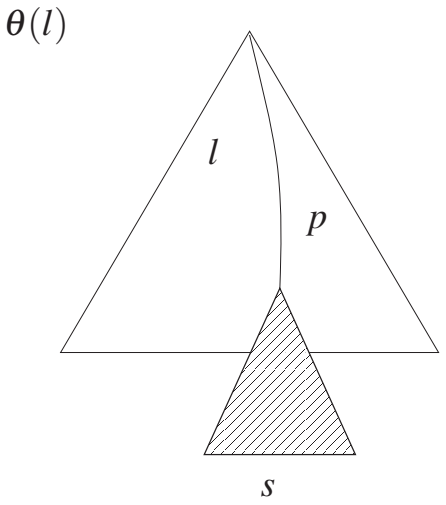

Figure 6.1: *s*-overlap of l and t at position p

Example 6.0.19. *Let $\phi = \nu\tilde{n}.\sigma = \nu\{a\}.\{X_1 \mapsto g_1(a)\}$ be a frame and let*

$$R_1 = \{f(g_1(x), h(x)) \to g_2(x)\}$$

where h is R_1-resistant. Then $f(g_1(a), h(a))$ is not an s-overlap since it is not a plat (i.e., we cannot construct $h(a)$ since a is in $\tilde{n}$).

Example 6.0.20. *Let $\phi = \nu\tilde{n}.\sigma = \nu\{a\}.\{X_1 \mapsto g_1(a)\}$ be a frame and let*

$$R_2 = \{f(g_1(x), h(x,y)) \to g_2(x)\}$$

where h is R_2 transparent. Then the only s-overlap is $f(g_1(a), h(a,y))$. Which has no instance that is a plat.

Note that when R is Δ-strong, $\theta(r)$ will be a ground term and besides $\theta(r) \prec \theta(l|_p) = t$. This fact is crucial in many of the following proofs.

Lemma 6.0.21. *Let R be a convergent term rewriting system and let $\phi = \nu\tilde{n}.\sigma$ be a frame where σ is an $\mathscr{I}$-independent substitution and the root symbol of every term in $\mathscr{R}an(\sigma)$ is R-resistant. Let $t \in T_\phi$ be an irreducible recipe such that $\sigma(t)$ is a redex. Then there is an s-overlap S such that $\sigma(t)$ is an instance of S.*

Proof. Let $l \to r$ be a rule in R such that $l \lesssim \sigma(t)$, i.e., $\exists\theta :\ \theta(l) = \sigma(t)$. Thus $\mathscr{P}os(l) \subseteq \mathscr{P}os(\sigma(t))$. By Lemma 4.0.16 we know that $\mathscr{P}os(l) \not\subseteq \mathscr{P}os(t)$, since otherwise t would be reducible. Thus there must exist a position $p \in \mathscr{FP}os(l)$ and a variable $X_j \in \mathscr{V}ar(t)$ such that $\theta(l|_p) = \sigma(X_j)$, i.e., $l|_p \lesssim \sigma(X_j)$. Let $\eta = mgu(l|_p =^? \sigma(X_j))$. Thus $\eta \lesssim \theta$. By Definition 19 we have that $\eta(l)$ is the s-overlap of l and $\sigma(X_j)$ at position p and the result follows. □

Note, that in our co-saturation procedure we will refer to ψ as a "parallel universe", in the sense that ψ is where the intruder can try to extend his knowledge by applying cryptographic primitives and making guesses on keys. Informally our goal is to compare these two "universes" or frames at various stages as they evolve over time during our procedures.

In the other cases, where the substitutions need not be extended because the terms are already in the range of σ, we need to check whether the recipes produce the 'mirror' terms in the range of ρ. More precisely, in the overlapping case, if there is already a mapping $(x_j \mapsto \theta(r))$, then we have to check whether $(x_j \mapsto \widehat{t})$ is in ρ. Similarly, in the dismantling case if there is a mapping $(x_j \mapsto s_i)$ in σ, then we should check whether the mapping $\left(x_j \mapsto (C_i^g[\rho(x_i)])\downarrow_R\right)$ is in ρ. (Thus the cover-set has to be constructed in any case.)

An easy way to picture what we are doing with our co-saturation procedure is to relate it to the Marx brothers' 1933 film "Duck Soup". In this film there is an well-known scene involving Groucho and Harpo. In this scene Harpo pretends to be Groucho's reflection. Groucho starts out being suspicious of his reflection and begins doing elaborate moves that Harpo must predict and try to mimic as to not raise suspicion. Some of these moves start off screen and many involve props such as hats. Groucho is often fooled by

The key ideas of the modified co-saturation procedure are as follows. There are two cases, which we refer to as the *overlapping* case and the *dismantling* case respectively, where we extend the substitutions:

$\dfrac{s \in \mathscr{R}an(\sigma) \qquad (l,p)}{\sigma \cup \{x_{n+1} \mapsto \theta(r)\}}$	if $\theta = mgu(l|_p =^? s)$ where $\theta(r) \notin \mathscr{R}an(\sigma)$ and root(s) is R-resistant, then we compute the cover-set $\mathscr{S}_c$ of $\theta(l)$, apply the substitution ρ of frame ψ (i.e., our parallel universe) to terms in this set, and then check if all terms in $\rho(\mathscr{S}_c)$ have the same *ground* normal form, i.e., whether $\rho(\mathscr{S}_c)\downarrow_R$ is a singleton set of ground terms. If it is, say $\{\widehat{t}\}$, then set $\rho = \rho \cup \{x_{n+1} \mapsto \widehat{t}\}$, where $n = |\mathscr{D}om(\sigma)|$; if it is not then $\phi \not\sqsubseteq_S \psi$.
$\dfrac{(X \mapsto g(s_1,\ldots,s_m)) \in \sigma}{\sigma \cup \{x_{n+1} \mapsto C_i^g[s]\}}$	if g is R-transparent and $s_i \notin \mathscr{R}an(\sigma)$, where $1 \leq i \leq m$ and $n = |\mathscr{D}om(\sigma)|$. We extend ρ by adding $x_{n+1} \mapsto (C_i^g[\rho(x_i)])\downarrow_R$.

Note that the main check that is performed during this procedure is determining if $\rho(\mathscr{S}_c)\downarrow_R$ is a singleton set of ground terms.

Harpo wearing props that are the wrong color and even when Harpo switches places with him "inside the mirror". He is nearly convinced that Harpo is his reflection until Chico wanders into the scene and bumps into both Harpo and Groucho. This scene relates to our procedure in many ways. Consider that Groucho is ϕ and Harpo is ψ. In our procedure if ψ is a clever "mimicker" then ϕ may still be deceived into thinking that it is statically included in ψ even after our procedure terminates. Thus we must perform additional checks to ensure that ϕ has not been fooled by clever "mimicking."

We will formulate our co-saturation procedure in Figure 1. Please note that even if the co-saturation exits without failure we cannot deduce that ϕ is statically included in ψ yet.

Let $n = |\mathscr{D}om(\sigma)| = |\mathscr{D}om(\rho)|$.

1. For every mapping $X \mapsto g(s_1,\ldots,s_m)) \in \sigma$, where g is R-transparent,

   - for $i = 1,\ldots,n$:

     i. if $s_i \notin \mathscr{R}an(\sigma)$, we set $\sigma = \sigma \cup \{x_{n+1} \mapsto s_i\}$ and $\rho = \rho \cup \{x_{n+1} \mapsto (C_i^g[\rho(x_i)])\downarrow_R\}$.

     ii. if there is a mapping $(x_j \mapsto s_i)$ in σ, then check whether the mapping $(x_j \mapsto (C_i^g[\rho(x_i)])\downarrow_R)$ is in ρ. If so, continue; if not, output "Not included".

2. For every mapping $X \mapsto s$ where root(s) is R-resistant, rule $l \to r$ and position $p \in \mathscr{FP}os(l)$ such that $l|_p$ and s are unifiable, let $\theta = mgu(l|_p =^? s)$, $\mathscr{S}_c$ = the cover-set of $\theta(l)$ and $\mathscr{U} = \rho(\mathscr{S}_c)\downarrow_R$. Now if $\mathscr{U}$ is not a singleton set of ground terms, then output "Not included". If it is, say $\{\widehat{t}\}$, then

   - if $\theta(r) \notin \mathscr{R}an(\sigma)$, then set $\sigma = \sigma \cup \{x_{n+1} \mapsto \theta(r)\}$ and $\rho = \rho \cup \{x_{n+1} \mapsto \widehat{t}\}$.

   - if there is already a mapping $(x_j \mapsto \theta(r))$ in σ, then check whether $(x_j \mapsto \widehat{t})$ in ρ. If so, continue; if not, output "Not included".

Figure 6.2: Saturation Procedure

Definition 20. *We say that two frames $\phi = \nu\tilde{n}.\sigma$ and $\psi = \nu\tilde{n}'.\rho$ are co-saturated if and only if σ does not grow under any application of our inference rules and we have encountered no failures.*

Note that though we call our procedure a co-saturation procedure we are only actually saturating frame ϕ. In ψ we are just mirroring the effects of ϕ being saturated.

Lemma 6.0.22. *Let R be a convergent term rewriting system and let* $\phi = \nu\tilde{n}.\sigma$ *and* $\psi = \nu\tilde{n}.\rho$ *be co-saturated frames. If* $(X \mapsto g(t_1,\ldots,t_n)) \in \sigma$ *and g is transparent, then* $(X \mapsto g(t_1,\ldots,t_n))$ *does not belong to the* $\mathscr{I}$*-core of* σ.

Proof. Straightforward, since the dismantling step will add mappings of the form $X_{j_i} \mapsto t_i$ (unless t_i is already in $\mathscr{R}an(\sigma)$) for $1 \leq i \leq n$. □

Lemma 6.0.23 (Soundness and completeness)**.** *Let R be a convergent term rewriting system and let* $\phi = \nu\tilde{n}.\sigma$ *and* $\psi = \nu\tilde{n}.\rho$ *be co-saturated frames. Then* $\phi \sqsubseteq_S \psi$ *if and only if every mapping in* σ *not in its* $\mathscr{I}$*-core is syntactically redundant with respect to* ρ.

Proof. For ease of exposition, we partition σ as follows:

$$\sigma = \sigma_c \uplus \sigma_{nc}$$

where σ_c is the $\mathscr{I}$-core of σ and σ_{nc} is the remainder of σ. Let $\phi_c = \nu\tilde{n}.\sigma_c$.

Proof (only-if). We will prove this by contradiction. We will assume that $\phi \sqsubseteq_S \psi$ and that there exists a mapping $(X \mapsto s)$ in σ_{nc} that is not syntactically redundant with respect to ρ. Since σ_c is the $\mathscr{I}$-core of σ there must be a recipe τ_s such that $s = \sigma_c(\tau_s)$. Thus it must be that $\rho(X)$ and $\rho(\tau_s)$ are not joinable modulo R. This contradicts the assumption that $\phi \sqsubseteq_S \psi$. □

Proof (if). If every mapping in σ_{nc} is syntactically redundant with respect to ρ then $\phi \sqsubseteq_S \psi$. We prove this by contradiction. Let t_1, t_2 be a minimal counterexample (i.e., $\sigma_c(t_1) \downarrow_R \sigma_c(t_2)$ whereas $\rho(t_1)$ and $\rho(t_2)$ are not joinable) with respect to the number of steps in their *joinability sequence,* i.e., $\sigma_c(t_1) \xrightarrow{j} z \xleftarrow{k} \sigma_c(t_2)$ so their joinability sequence is $j+k$ steps. We assume that σ is a normalized substitution and that t_1 and t_2 are irreducible recipes. Since σ_c is an $\mathscr{I}$-independent substitution it has to be that $j+k > 0$, by Lemma 4.0.15. Without loss of generality, we assume that $j > 0$, i.e., $\sigma_c(t_1)$ is reducible. Let t_3 be a non-ground subterm of t_1 such that $\sigma_c(t_3)$ is a redex and let q be its position in t_1, i.e., $t_3 = t_1|_q$.

By Lemma 6.0.21 we know that an s-overlap S exists such that $\sigma_c(t_3)$ is an instance of S. Thus, we know that there exists a rule $l \to r \in R$, a mapping $X \mapsto s$ and a substitution $\theta = mgu(l|_p =^? s)$ where $p \in \mathscr{FP}os(l)$, such that $\theta(l) = \mathsf{S}$. So $\sigma_c(t_3) \downarrow_R = \theta(r)$. Since ϕ is saturated, $\theta(r)$ is either in $\mathscr{R}an(\sigma_c)$ or in $\mathscr{R}an(\sigma_{nc})$.

(a) $\theta(r) \in \mathscr{R}an(\sigma_c)$: Then there exists a variable $Y \in \mathscr{D}om(\sigma_c)$ such that $\sigma_c(Y) = \theta(r)$.

(b) $\theta(r) \in \mathscr{R}an(\sigma_{nc})$: In this case, due to redundancy, there exists a ϕ_c-recipe τ such that $\sigma_c(\tau) = \theta(r)$.

Thus we can say in general that there is a ϕ_c-recipe τ_r such that $\theta(r) = \sigma_c(\tau_r)$. Let $t_1' = t_1[\tau_r]_q$. By doing this replacement we know that we have effectively done a reduction in $\sigma_c(t_1)$ since we have reduced its subterm $\sigma_c(t_3)$ to a ground plat. Thus $\sigma_c(t_1) \to_R^+ \sigma_c(t_1[\tau_r]_q) = \sigma_c(t_1')$ and we have decreased j by at least one step. Therefore the length of the joinability sequence for t_1' and t_2 is now $(j-m)+k$ where $m \geq 1$. However this contradicts the minimality of t_1 and t_2 since we have now found a pair with a shorter joinability sequence which is a smaller counterexample. □

Recall Example 1.1.2 from Chapter 1. We will now define this example more formally and use our procedure to show that $\phi \sqsubseteq_S \psi$.

Example 6.0.24. *Let our term rewriting system R be:*

$$R = \{d(e(x,y),y) \to x,\ \pi_1(p(x,y)) \to x,\ \pi_2(p(x,y)) \to y\}$$

and let ϕ and ψ be frames such that

$$\phi = \nu\tilde{n}.\sigma = \nu\{M,N_a,q,q',K\}.\{X_1 \mapsto e(N_a,q),\ X_2 \mapsto e(p(M,N_a),K),\ X_3 \mapsto q\}$$

and

$$\psi = \nu\tilde{n}.\rho = \nu\{M,N_a,q,q',K\}.\{X_1 \mapsto e(N_a,q),\ X_2 \mapsto e(p(M,N_a),K),\ X_3 \mapsto q'\}.$$

Consider, $\theta = mgu(d(e(x,y),y)|_1 =^? e(p(M,N_a),K))$*, then* $\theta(l) = d(e(p(M,N_a),K)K)$ *is not an s-overlap since it is not a plat (i.e., we cannot construct K since K is in* $\tilde{n}$*). But if,* $\theta = mgu(d(e(x,y),y)|_1 =^? e(N_a,q)$*, then* $\theta(l) = d(e(N_a,q),q)$ *is an s-overlap since it has an instance* $d(X_1,X_3)$ *which is a* ϕ*-plat and* $\theta(r) = N_a \notin \mathscr{R}an(\sigma)$*.*
The pre-cover-set of $\theta(l)$ *is*

$$\text{pre-cover-set}(\theta(l)) = \{d(e(N_a,q),q)\}$$

The cover-set of $\theta(l)$ *is*

$$\mathscr{S}_c(\theta(l)) = \{d(X_1,X_3)\}$$

$$\mathscr{U} = \{\rho(d(X_1,X_3))\downarrow_R\} = \{d(e(N_a,q),q')\}$$

Since $\mathscr{U}$ *is a ground singleton set we extend* ρ *and* σ *as follows:*

$$\sigma = \{X_1 \mapsto e(N_a,q),\ X_2 \mapsto e(p(M,N_a),K),\ X_3 \mapsto q,\ X_4 \mapsto N_a\}$$

$$\rho = \{X_1 \mapsto e(N_a,q),\ X_2 \mapsto e(p(M,N_a),K),\ X_3 \mapsto q',\ X_4 \mapsto d(e(N_a,q),q')\}$$

We can no longer apply any inference rules, since there are no more valid s-overlaps. Thus our frames are co-saturated.

The $\mathscr{I}$*-core of* σ *is* $\{X_2 \mapsto e(p(M,N_a),K),\ X_3 \mapsto q,\ X_4 \mapsto N_a\}$*. The mapping* $X_1 \mapsto e(N_a,q)$ *is syntactically redundant in* ρ*, since*

$$X_1 = \sigma(e(X_4,X_3))$$

and

$$\rho(e(X_4,X_3)) = e(d(e(N_a,q),q'),q') \rightarrow_R^! e(N_a,q) = \rho(X_1).$$

By Lemma 6.0.23 we conclude that $\phi \sqsubseteq_S \psi$*.*

Lemma 6.0.25. *Any frames* $\phi = \nu\tilde{n}.\sigma$ *and* $\psi = \nu\tilde{n}.\rho$ *can be co-saturated in a finite number of steps.*

Proof by contradiction. Assume there is an infinite chain of co-saturation steps. This must involve the overlapping case, since the dismantling case simply "strips off" root

symbols leaving smaller terms at every step which will clearly terminate. Thus the infinite chain must involve computing the cover set of valid s-overlaps. We can build a finitely branching infinite tree from nodes that represent all of the terms in $\mathscr{R}an(\sigma)$ as follows:

- The root of the tree will be an arbitrary symbol not in $(F \cup \texttt{Names})$.
- The level $i = 1$ of the tree will be all the terms in $\mathscr{R}an(\sigma)$.
- The $i+1$ level of the tree is obtained from applying our inference rule to all of the terms $s \in \mathscr{R}an(\sigma)$ in the i^{th} level. If a new mapping is added to σ by an s-overlap $\theta(l)$ of l and s at p, then the corresponding $\theta(r)$ becomes a child of s in the tree. Recall that since R is a Δ-strong rewrite system we know that $\theta(r) \prec \theta(l|_p)$.

This tree is clearly finitely branching since for each node in the tree we can only match at most with $l|_p$ for every $l \to r \in R$ and every $p \in \mathscr{FP}os(l)$. By König's Lemma we know that this tree must have an infinite path. However, this is impossible since each term that is added must be lower than it's parent in the ordering $\prec$. Thus we have reached our contradiction and no infinite chain of co-saturation steps can exist. □

Example 6.0.26. *Let* $R = \{d(e(x,y),y) \to x\}$. *Let*

$$\phi = \nu\tilde{n}.\sigma = \nu\{k,k_1\}.\{X_1 \mapsto e(a,k),\ X_2 \mapsto k\}$$

and

$$\psi = \nu\tilde{n}.\rho = \nu\{k,k_1\}.\{X_1 \mapsto e(a,k),\ X_2 \mapsto k_1\}$$

be frames.
The s-overlap is

$$\theta(l) \ = \ d(e(a,k),k)$$

Note that $\theta(l) = \sigma(d(X_1,X_2))$, *thus* $\theta(l)$ *is a* ϕ*-plat and* $\theta(r) = a \notin \mathscr{R}an(\sigma)$.
The cover-set of $\theta(l)$ *is*

$$\mathscr{S}_c(\theta(l)) = \{d(X_1,X_2)\}$$

$$\mathscr{U} = \{\rho(d(X_1,X_2))\downarrow_R\} = \{d(e(a,k),k_1)\}$$

Since $\mathscr{U}$ is a ground singleton set we extend ρ and σ as follows:

$$\sigma = \{X_1 \mapsto e(a,k),\ X_2 \mapsto k,\ X_3 \mapsto a\}$$

$$\rho = \{X_1 \mapsto e(a,k),\ X_2 \mapsto k_1,\ X_3 \mapsto d(e(a,k),k_1)\}$$

The $\mathscr{I}$-core of σ is $\{X_2 \mapsto k\}$ since a is a public constant. The mapping $X_1 \mapsto e(a,k)$ is not in $\mathscr{I}$-core of σ and is not syntactically redundant in ρ, since $X_1 = \sigma(e(a,X_2))$ and $\rho(X_1) \neq_R \rho(e(a,X_2))$. Thus by Lemma 6.0.23 $\phi \not\sqsubseteq_S \psi$. (The mapping $X_3 \mapsto a$ is not redundant either.)

Example 6.0.27. *(A small variation of Example 6.0.26)*

Let $R = \{d(e(x,y),y) \to x,\ e(d(x,y),y) \to x\}$ and let

$$\phi = \nu\tilde{n}.\sigma = \nu\{a,k,k_1\}.\{X_1 \mapsto e(a,k),\ X_2 \mapsto k\}$$

and

$$\psi = \nu\tilde{n}.\rho = \nu\{a,k,k_1\}\,.\,\{X_1 \mapsto e(a,k),\ X_2 \mapsto k_1\}$$

be frames. Saturation yields the same substitutions as before:

$$\sigma = \{X_1 \mapsto e(a,k),\ X_2 \mapsto k,\ X_3 \mapsto a\}$$

$$\rho = \{X_1 \mapsto e(a,k),\ X_2 \mapsto k_1,\ X_3 \mapsto d(e(a,k),k_1)\}$$

The $\mathscr{I}$-core of σ is $\{X_2 \mapsto k,\ X_3 \mapsto a\}$. The mapping $X_1 \mapsto e(a,k)$ now is syntactically redundant in ρ, since

$$X_1 = \sigma(e(X_3,X_2))$$

and

$$\rho(e(X_3,X_2) = e(d(e(a,k),k_1),k_1) \to_R^! e(a,k) = \rho(X_1)$$

Example 6.0.28. *Let $R = \{f(g(x),y) \to h(x)\}$ and let*

$$\phi = \nu\tilde{n}.\sigma = \nu\{a\}\,.\,\{X_1 \mapsto g(a)\}$$

and

$$\psi = \nu\tilde{n}.\rho = \nu\{a\}\,.\,\{X_1 \mapsto h(a)\}$$

be frames.

Consider that the s-overlap is $\theta(l) = f(g(a),y)$. *Note that* $\theta(l) = \sigma(f(X_1,y))$, *thus* $\theta(l)$ *is a* ϕ*-plat and* $\theta(r) = h(a) \notin \mathscr{R}an(\sigma)$.

The cover-set of $\theta(l)$ *is*

$$\mathscr{S}_c(\theta(l)) = \{f(X_1,y)\}$$

$\mathscr{U} = \rho(\{f(X_1,y)\})\downarrow_R = \{f(h(a),y)\}$. *Since* $\mathscr{U}$ *is not a ground singleton set,* $\phi \not\sqsubseteq_S \psi$.

Example 6.0.29. *Let* $R = \{f(g(x,y),g(x,z)) \to h(x)\}$ *and let*

$$\phi = \nu\tilde{n}.\sigma = \nu\{a,b,c,d,d'\}\,.\,\{X_1 \mapsto g(a,b), X_2 \mapsto g(a,c)\}$$

and

$$\psi = \nu\tilde{n}.\rho = \nu\{a,b,c,d,d'\}\,.\,\{X_1 \mapsto g(d,b), X_2 \mapsto g(d',c)\}$$

be frames.

The s-overlap is

$$\theta(l) = f(g(a,b),g(a,z)).$$

Note that $\{z \mapsto b\}(\theta(l)) = \sigma(f(X_1,X_1))$, *thus* $\theta(l)$ *has an instance that is a* ϕ*-plat.*

Therefore we know that $\theta(r) = \theta(h(x)) = h(a) \notin \mathscr{R}an(\sigma)$.

The cover-set of $\theta(l)$ *is*

$$\mathscr{S}_c(\theta(l)) = \{f(X_1,X_1),\ f(X_1,X_2)\}$$

and

$$\mathscr{U} = \rho(\{f(X_1,X_1),\ f(X_1,X_2)\})\downarrow_R = \{h(d),\ f(g(d,b),g(d',c))\}.$$

Since $\mathscr{U}$ *is not a ground singleton set, we conclude that* $\phi \not\sqsubseteq_S \psi$.

CHAPTER 7
$\omega\nabla$-strong Intruder Theories

Now we shall look at a more general class of theories known as $\omega\nabla$-strong intruder theories[1]. We will provide a new co-saturation procedure for deciding this class of theories. Note that as in the previous chapter our procedure is an algorithm for solving the static inclusion decision problem, however for a more general class of intruder theories.

We will begin by defining an $\omega\nabla$-strong intruder theory.

Definition 21. *Let $\succ$ be a simplification ordering on the term rewriting system R, and Δ a dwindling and convergent subsystem of R. For every rule $l \to r$ in R, let $\mu(l)$ stand for the set of $\succ$-minimal subterms of l that are R-resistant. A rule $l \to r \in R$ is said to be ω-strong with respect to $\succ$, if and only if there exists a position p such that $l|_p \in \mu(l)$ and $l|_p \succ r$. The system R is $\omega\nabla$-strong with respect to $\succ$, if and only if every rule in R is either dwindling or ω-strong with respect to $\succ$.*

Clearly every Δ-strong term rewriting system is also $\omega\nabla$-strong. An example of a term rewriting system that is dwindling (and hence $\omega\nabla$-strong) but not Δ-strong is

$$\Big\{ d(e(x, pk(y)),\ sk(y)) \to x \Big\}$$

for public-key encryption and decryption. (Note that *sk* is *R*-resistant.)

[1]Note that in "Intruder with caps" [6] they did not study $\omega\nabla$-strong intruder theories. Instead that paper studied a related class of theories known as $\omega\Delta$-strong intruder theories, which is slightly different because not every function symbol is public. Nevertheless, our approach is clearly inspired by [6].

Now we shall present our new co-saturation procedure. We will provide a more generalized version of the overlapping case from the previous section.

$\dfrac{s \in \mathscr{R}an(\sigma) \qquad (l,p)}{\sigma \cup \{x_{n+1} \mapsto \theta(r)\}}$	if $\theta = mgu(l|_p =^? s)$ where root(s) is R-resistant, $\theta(r) \notin \mathscr{R}an(\sigma)$ and $\boxed{s \succ \theta(r)}$, then we compute the cover-set $\mathscr{S}_c$ of $\theta(l)$, apply the substitution ρ of frame ψ (i.e., our parallel universe) to terms in this set, and then check if all terms in $\rho(\mathscr{S}_c)$ have the same *ground* normal form, i.e., whether $\rho(\mathscr{S}_c)\downarrow_R$ is a singleton set of ground terms. If it is, say $\{\widehat{t}\}$, then set $\rho = \rho \cup \{x_{n+1} \mapsto \widehat{t}\}$, where $n = |\mathscr{D}om(\sigma)|$; if it is not then $\phi \not\sqsubseteq_S \psi$.
$\dfrac{(X \mapsto g(s_1,\ldots,s_m)) \in \sigma}{\sigma \cup \{x_{n+1} \mapsto C_i^g[s]\}}$	if g is R-transparent and $s_i \notin \mathscr{R}an(\sigma)$, where $1 \leq i \leq m$ and $n = |\mathscr{D}om(\sigma)|$. We extend ρ by adding $x_{n+1} \mapsto (C_i^g[\rho(x_i)])\downarrow_R$.

As before, if there is already a mapping $(x_j \mapsto \theta(r))$ in σ, then we have to check whether $(x_j \mapsto \widehat{t})$ is in ρ. The dismantling case from the previous section needs no change.

Lemma 7.0.30. *Let R be a convergent term rewriting system and let $\phi = \nu\tilde{n}.\sigma$ be a frame where σ is an $\mathscr{I}$-independent substitution and the root symbol of every term in $\mathscr{R}an(\sigma)$ is R-resistant. Let $l \to r$ be a rule in R that is ω-strong and $p \in \mathscr{F}Pos(l)$ such that $l|_p \in \mu(l)$ and $l|_p \succ r$. If, for some substitution θ, $\theta(l|_p)$ is a ϕ-plat and $\theta(r)$ is not, then $\theta(l|_p) \in \mathscr{R}an(\sigma)$.*

Proof. Since $\theta(r)$ is not a plat, there must be a variable v in $\mathscr{V}ar(r)$ and hence in $\mathscr{V}ar(l|_p)$ such that $\theta(v)$ is not a plat. Thus $\theta(v)$ is not a plat whereas a superterm of it, namely $\theta(l|_p)$, is a plat. Let $p \cdot p'$ be a position of v in l. By Corollary 3.0.5, there must be a position q such that $p \preceq q \prec p \cdot p'$ and $\theta(l|_q) \in \mathscr{R}an(\sigma)$, or, in other words, $\theta(v)$ must be a *proper* subterm of some term in $\mathscr{R}an(\sigma)$ which, in turn, must be a subterm of $\theta(l|_p)$. Let $s = \theta(l|_q)$. Now, $l|_p$ is a *minimal* R-resistant subterm of l, so all function symbols of $l|_p$, except at its root, must be R-transparent; but the root of s is R-resistant by our assumption above, so it must be that $\theta(l|_p)$ is a subterm of s; thus $\theta(l|_p) \in \mathbf{ST}(\mathscr{R}an(\sigma))$.

But since $\theta(l|_p)$ is a plat, it must be *in* $\mathscr{R}an(\sigma)$. □

We can now provide a more general form of this lemma as follows:

Lemma 7.0.31. *Let R be a convergent term rewriting system and let* $\phi = \nu\tilde{n}.\sigma$ *be a frame where* σ *is an* $\mathscr{I}$*-independent substitution and the root symbol of every term in* $\mathscr{R}an(\sigma)$ *is R-resistant. Let* $l \to r$ *be a rule in R that is* ω*-strong and* $p \in \mathscr{F}Pos(l)$ *such that* $l|_p \in \mu(l)$ *and* $l|_p \succ r$*. If, for some substitution* θ*,* $\theta(l)$ *is a* ϕ*-plat and* $\theta(r)$ *is not, then there is a prefix q of p such that* $\theta(l|_q) \in \mathscr{R}an(\sigma)$*.*

Proof. If $\theta(l|_p)$ is a ϕ-plat, then the result follows from Lemma 7.0.30. If it is not, then Corollary 3.0.5 applies, since $\theta(l|_p) = \theta(l)|_p$. □

Lemma 7.0.32. *Let R be a convergent term rewriting system and let* $\phi = \nu\tilde{n}.\sigma$ *be a frame where* σ *is an* $\mathscr{I}$*-independent substitution and the root symbol of every term in* $\mathscr{R}an(\sigma)$ *is R-resistant. Let* $l \to l|_p$ *(*$p \neq \varepsilon$*) be a dwindling rule in R. If, for some substitution* θ*,* $\theta(l)$ *is a* ϕ*-plat and* $\theta(l|_p)$ *is not, then there exists a position* $\varepsilon \preceq q \prec p$ *such that* $\theta(l|_q) \in \mathscr{R}an(\sigma)$*.*

Proof. Follows from Corollary 3.0.5. □

Lemma 7.0.33. *Let R be a convergent term rewriting system that is* $\omega\triangledown$*-strong and let* $\phi = \nu\tilde{n}.\sigma$ *be a frame where* σ *is an* $\mathscr{I}$*-independent substitution and the root symbol of every term in* $\mathscr{R}an(\sigma)$ *is R-resistant. Let* t, t' *be terms such that* $t \to_R t'$ *where t is both a plat as well as a redex. If* t' *is not a plat, then there is an s-overlap* S *such that t is an instance of* S*.*

Proof. Let $l \to r$ be a rule in R, such that $\theta(l) = t$ and $\theta(r) = t$ for some substitution θ. Since $l \to r$ is $\omega\triangledown$-strong we must consider the following cases:

Case 1 Let $l \to r$ is a dwindling rule. We know that $\theta(l)$ is a plat and $\theta(l|_p)$ is not a plat where $p \in \mathscr{F}\mathscr{P}os(l)$ $l|_p$ can be replaced by r since $l \to r$ is dwindling. Thus there must exist a position q where q is a proper prefix of p and $\theta(l|_q) \in \mathscr{R}an(\sigma)$ by Lemma 7.0.32.

Case 2 Let $l \to r$ is an ω-strong rule. Thus by by Lemma 6.0.21 there must exist a position $p \in \mathscr{FP}os(l)$ such that $l|_p \in \mu(l)$, $l|_p \succ r$, q is a prefix of p and $\theta(l|_q) \in \mathscr{R}an(\sigma)$.

Therefore in both cases we know there is an s-overlap S such that t is an instance of S by Lemma 6.0.21. Now what remains to be shown is that $\theta(l|_q) \succ \theta(r)$. This is clear since $l|_q$ is a prefix of $l|_p$ where $l|_p \succ r$. Therefore $\theta(l|_q) \succ \theta(r)$. □

Lemma 7.0.34. *Let R be a convergent term rewriting system that is $\omega\triangledown$-strong and let $\phi = \nu\tilde{n}.\sigma$ be a frame where σ is an $\mathscr{I}$-independent substitution and the root symbol of every term in $\mathscr{R}an(\sigma)$ is R-resistant. Let t, t' be terms such that $t \to_R t'$ where t is both a plat as well as a redex. If t' is a plat, then there is an equation $e_1 = e_2$ in the cover-set of R such that $t = t'$ is an instance of $e_1 = e_2$.*

Proof. Let $l \to r$ be a rule in R such that $\sigma(l) = t$ and $\sigma(r) = t'$. The cover-set of R is, by definition, a superset of the cover-set of $l = r$. Now the result follows from the definition of cover-set (Lemma 3.0.10). □

Note that the termination argument given in Lemma 6.0.25 with slight modifications will work for $\omega\triangledown$-strong intruder theories as well.

Theorem 7.0.35 (Soundness and completeness)**.** *Let R be a convergent term rewriting system that is $\omega\triangledown$-strong. Let $\phi = \nu\tilde{n}.\sigma$ and $\psi = \nu\tilde{n}.\rho$ be co-saturated frames and $\phi_c = \nu\tilde{n}.\sigma_c$ be the $\mathscr{I}$-core of ϕ. Then $\phi \sqsubseteq_S \psi$ if and only if the following hold:*

1. *every mapping in σ not in its $\mathscr{I}$-core is syntactically redundant with respect to ρ, and*
2. *every equality in the cover-set for R with respect to ϕ_c also holds in ψ.*

Proof. For ease of exposition, we partition σ as follows:

$$\sigma = \sigma_c \uplus \sigma_{nc}$$

Proof (only if). We will prove this by contradiction. We will assume $\phi \sqsubseteq_S \psi$ and there exists a mapping $(X \mapsto s)$ in σ_{nc} that is not syntactically redundant with respect to ρ.

Since σ_c is the $\mathscr{I}$-core of σ there must be a recipe τ_s such that $s = \sigma_c(\tau_s)$. Thus it must be that $\rho(X)$ and $\rho(\tau_s)$ are not joinable modulo R. This contradicts the assumption that $\phi \sqsubseteq_S \psi$. □

Proof (if). We prove that if the conditions hold then $\phi \sqsubseteq_S \psi$. We first prove the following claim:

> **Claim**: If, for some substitution θ, $\theta(l)$ is a ϕ-plat, then so is $\theta(r)$.
>
> *Proof by contradiction.* Suppose $\theta(l)$ is a ϕ-plat and $\theta(r)$ is not a ϕ-plat. Thus by Lemma 7.0.33 we know that there is an s-overlap S such that $\theta(l)$ is an instance of S. Therefore we will be able to extend our substitution σ by applying our overlapping rule. However this is a contradiction since we know that our frames are already co-saturated. □

We now prove the "if" part by contradiction. Let t_1, t_2 be a minimal counterexample (i.e., $\sigma_c(t_1) \downarrow_R \sigma_c(t_2)$ whereas $\rho(t_1)$ and $\rho(t_2)$ are not joinable) with respect to the number of steps in their *joinability sequence,* i.e., $\sigma_c(t_1) \xrightarrow{j} z \xleftarrow{k} \sigma_c(t_2)$ so the length of their joinability sequence is $j+k$ steps. We assume that σ is a normalized substitution and that t_1 and t_2 are irreducible recipes. Since σ_c is an $\mathscr{I}$-independent substitution it has to be that $j+k > 0$, by Lemma 4.0.15. Without loss of generality, we assume that $j > 0$, i.e., $\sigma_c(t_1)$ is reducible. Let t_3 be a non-ground subterm of t_1 such that $\sigma_c(t_3)$ is the first redex in the reduction sequence and let q be its position in t_1, i.e., $t_3 = t_1|_q$. Thus there is a rule $l \to r \in R$ such that $\sigma_c(t_3) = \theta(l)$. Note that by our above claim we know that $\theta(r)$ must also be a ϕ-plat and hence a ϕ_c-plat. By Lemma 7.0.34 there is an equation $e_l = e_r$ in the cover-set of R with respect to ϕ_c such that $\theta(l) =_R \theta(r)$ is an instance of it. Therefore $\theta(r) = \eta(\sigma_c(e_r))$ where $\eta \uplus \sigma_c$ is a plat extension of σ_c. Since $\eta(\sigma_c(e_r)) = \sigma_c(\eta(e_r))$[2] we can set $t_3' = \eta(e_r)$. Similarly for $\theta(l)$ we have that $\theta(l) = \sigma_c(\eta(e_l))$ where $\eta(e_l)$ must be equal to t_3 by Lemma 4.0.15. Note that t_3 and t_3' are equivalent with respect to ρ too, since $e_l = e_r$ holds in ψ.

Let $t_1' = t_1[t_3']_q$. By doing this replacement we have effectively done a reduction in $\sigma_c(t_1)$ since we have reduced its subterm $\sigma_c(t_3)$ to a ground plat. Thus $\sigma_c(t_1) \to_R^+$

[2]Since i.e., η and σ_c are ground substitutions with different domains

$\sigma_c(t_1[t'_3]_q) = \sigma_c(t'_1)$ and we have decreased j by at least one step. Therefore the joinability sequence for t'_1 and t_2 is now $(j-m)+k$ where $m \geq 1$. However this contradicts the minimality of t_1 and t_2 since we have now found a pair with a shorter joinability sequence which is a smaller counterexample. □

CHAPTER 8
Conclusion and Future Work

In conclusion, the main contributions that we have made in this dissertation are providing co-saturation procedures for deciding if a frame ϕ is statically included in another frame ψ over specific classes of intruder theories. We developed our approach by essentially starting where "Intruders with Caps" ended. In that paper the authors were studying a related problem, the cap or deduction problem. They solved this problem for Δ-strong and $\omega\Delta$-strong intruder theories. We modified their procedures to solve the decision problem for static inclusion over Δ-strong and $\omega\triangledown$-strong theories. For these classes of theories we guarantee termination, soundness, and completeness.

A notion we introduced that was not in [6] is that of a cover-set. This was not needed in [6] because exactly how a term was deduced was not important there. Deciding the deduction problem was shown to be non-primitive recursive for general Δ-strong intruder theories [7]. The same proof can be adapted to show that deciding static inclusion is also of non-primitive recursive complexity over general Δ-strong intruder theories (see Appendix A).

As this dissertation is being written another more general approach is being developed. This approach uses a Knuth-Bendix style completion procedure [27]. As part of our future work we hope to complete this technique and if possible combine it with our approach. Another goal is to generalize our current technique to handle more classes of intruder theories. Additionally we would like to implement our co-saturation procedures and include them in a protocol analysis tool such as Maude-NPA [26]. We plan to provide detailed comparisons to other implementations such as YAPA [12], KiSs [23], and FAST [19].

APPENDIX A
Non-Primitive Recursive

With the permission of the authors [3, 31, 33], I will include material from an appendix in their *technical report* on "Intruders with Caps" [7]. This material was not in the published version of their paper [6]. We will show how to modify their construction to show that the complexity of deciding static inclusion over general Δ-strong intruder theories is non-primitive recursive.

The proof is based on the following lines of reasoning. The starting point is the following observation of Petr Jančar, where $\mathscr{A}(n)$ is a non-primitive recursive function on natural integers:

> "The problem to decide, given a 2-counter machine C and a natural number n, whether C halts on zero input in $\mathscr{A}(n)$ steps is non-primitive recursive".

in "*Nonprimitive recursive complexity and undecidability for Petri net equivalences*" (Theor. Comp. Science, 256(1-2):23–30, 2001; Proposition 9, Section 4).

Let C be an arbitrarily given 2-counter machine, with $L+1$ instructions; to each instruction of label i, $0 \leq i \leq L$, is associated a state denoted as q_i, which is treated as a unary function on $\mathbb{N}$. Consider the following convergent term rewriting system R, where 0 stands for the natural number 0, s for the successor function on $\mathbb{N}$, and p stands for the predecessor function defined as usual:

$$\begin{aligned}
f(0,x) &\rightarrow s(x)\\
f(s(x),0) &\rightarrow f(x,s(0))\\
f(s(x),s(y)) &\rightarrow f(x,f(s(x),y))\\
p(s(x)) &\rightarrow x\\
h(g(x,u,v,w)) &\rightarrow r(f(x,x),u,v,w)\\
d(q_i(x)) &\rightarrow x,\ \ 0 \leq i \leq L.
\end{aligned}$$

The function f obviously encodes the usual Ackermann-Peter function (on two

arguments over $\mathbb{N}$). The symbol h plays no specific role, other than ensuring that a term with top symbol g is R-irreducible. The q_i's and s are R-transparent and the other symbols are all R-resistant. Note that the last rule above is a meta-rule that represents a set of rewrite rules.

We encode the instructions of the given 2-counter machine C by the following set of rewrite rules, where the second and the fourth arguments, under the symbol r in the terms to the left, stand for the values of the two counters of C, respectively (and the l, l' are suitable instruction labels):

Incrementation of counter 1 or 2:

$$h(r(s(u),x,q_l(z),y)) \to r(u,s(x),q_{l+1}(z),y),$$

$$h(r(s(u),x,q_l(z),y)) \to r(u,x,q_{l+1}(z),s(y)).$$

Conditional decrementation of counter 1 or 2:

$$h(r(s(u),s(x),q_l(z),y)) \to r(u,x,q_{l+1}(z),y),$$

$$h(r(s(u),0,q_l(z),y)) \to r(u,0,q_{l'}(z),y).$$

$$h(r(s(u),x,q_l(z),s(y))) \to r(u,x,q_{l+1}(z),y),$$

$$h(r(s(u),x,q_l(z),0)) \to r(u,x,q_{l'}(z),0).$$

At STOP, release the secret m:

$$h(r(u,v,q_L(z),w)) \to z.$$

Let R' denote the intruder theory formed of all these encoding rules and the rules of the term rewriting system R given above; R' is obviously Δ-strong under the *lpo* based on the precedence $0 < q_i < s < p < f < r < g < h$ (where $0 \le i \le L$), and it is also convergent under this simplification ordering.

In [7] the authors show that a given ground constant m can be deduced from the singleton set $S = \{g(s^n(0), 0, q_0(m), 0)\}$, where n is some given positive integer, *if and only if* the machine C, with initial counter values both 0, halts under instruction L in $f(n,n)$ steps. Thus the deducibility problem for the Δ-strong intruder theory R' is non-primitive recursive.

Using an idea from [1], we show that this holds for the static inclusion problem as well. Let ϕ and ψ be frames defined as follows:

$$\phi \;=\; \nu\tilde{n}.\sigma \;=\; \nu\,\{m\}\,.\,\{X_1 \mapsto g(s^n(0), 0, q_0(m), 0),\; X_2 \mapsto d(m)\}$$

and

$$\psi \;=\; \nu\tilde{n}.\rho \;=\; \nu\,\{m\}\,.\,\{X_1 \mapsto g(s^n(0), 0, q_0(m), 0),\; X_2 \mapsto d(d(m))\}$$

where again n is some given positive integer, and m is a nonce.

Note that without the second mapping the two frames ϕ and ψ are identical; furthermore, we cannot have any s-overlaps with the second mapping, since the function symbol d only appears in the left-hand sides of the meta-rule (at the root) and none of the left-hand sides in this meta-rule can be matched with the range term $d(m)$. So, $d(m)$ is not in the $\mathscr{I}$-core after co-saturation if and only if m has been "deduced," i.e., a mapping of the form $X_i \mapsto m$ has been added. Clearly in this case $\phi \not\sqsubseteq_S \psi$.

Thus it is not hard to verify that $\phi \not\sqsubseteq_S \psi$ *if and only if* the machine C, with initial counter values both 0, halts in $f(n,n)$ steps. □

APPENDIX B
Some examples

1. Let $\sigma = \nu\{a\}.\{X_1 \mapsto g_1(a)\}$ be a frame.

   - $R_1 = \{f(g_1(x), h(y)) \to g_2(x)\}$ where h is transparent.
     The cover-set is $\{f(X_1, h(y))\}$.

   - $R_2 = \{f(g_1(x), h(x,y)) \to g_2(x)\}$ where h is transparent.
     The only s-overlap is $f(g_1(a), h(a,y))$.
     This has no instance that is a plat.

   - $R_3 = \{f(g_1(x), h(g_1(x), y)) \to g_2(x)\}$ where h is transparent.
     The s-overlap $f(g_1(a), h(g_1(a), y))$ has the cover-set $\{f(X_1, h(X_1, y))\}$.

   - $R_4 = \{f(g_1(x), h(g_1(y), y)) \to g_2(x)\}$ where h is transparent.
     (This system is not Δ-strong though.)
     The s-overlap $f(g_1(a), h(g_1(y), y))$ has the cover-set $\{f(X_1, h(g_1(y), y))\}$.
     Note that $f(X_1, h(X_1, a))$ is not a recipe.

2. Let $\sigma = \nu\{a\}.\{X_1 \mapsto g_1(a,a),\ X_2 \mapsto g_1(a,b)\}$ be a frame.

   - $R_5 = \{f(g_1(x,x),\ h(g_1(x,y), y)) \to g_2(x)\}$.
     Consider the s-overlap $f(g_1(a,a),\ h(g_1(a,y), y))$.
     Its cover-set is $\{f(X_1,\ h(X_2, b)\}$.
     Note that the instance $f(g_1(a,a),\ h(g_1(a,a), a))$ of the s-overlap is not a plat.

BIBLIOGRAPHY

[1] Martín Abadi and Véronique Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 367(1-2):2–32, 2006. 1.1, 1.2, A

[2] Martín Abadi and Cédric Fournet. Mobile values, new names, and secure communication. In Chris Hankin and Dave Schmidt, editors, *Conference Record of POPL 2001: The 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, London, UK, January 17-19, 2001*, pages 104–115. ACM, 2001. 1.2

[3] Siva Anantharaman. private communication, 2015. 1.2, A

[4] Siva Anantharaman, Christopher Bouchard, Paliath Narendran, and Michaël Rusinowitch. Unification modulo a 2-sorted equational theory for cipher-decipher block chaining. *Logical Methods in Computer Science*, 10(1), 2014. 6

[5] Siva Anantharaman, Hai Lin, Christopher Lynch, Paliath Narendran, and Michael Rusinowitch. Unification modulo homomorphic encryption. *Journal of Automated Reasoning*, 48(2):135–158, 2012. 6

[6] Siva Anantharaman, Paliath Narendran, and Michaël Rusinowitch. Intruders with caps. In Franz Baader, editor, *Term Rewriting and Applications, 18th International Conference, RTA 2007, Paris, France, June 26-28, 2007, Proceedings*, volume 4533 of *Lecture Notes in Computer Science*, pages 20–35. Springer, 2007. 1.1, 1.3, 2, 2, 6, 6, 1, 8, A

[7] Siva Anantharaman, Paliath Narendran, and Michaël Rusinowitch. Intruders with caps. Technical Report RR-2007-02, Laboratoire d'Informatique Fondamentale d'Orléans LIFO, 2007. 8, A

[8] Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. Analysing unlinkability and anonymity using the applied pi calculus. In *Proceedings of the 23rd Institute of*

Electrical and Electronics Engineers (IEEE) Computer Security Foundations Symposium, CSF 2010, Edinburgh, United Kingdom, July 17-19, 2010, pages 107–121. IEEE Computer Society, 2010. 1.2

[9] Franz Baader and Tobias Nipkow. *Term rewriting and all that*. Cambridge University Press, New York, NY, USA, 1998. 2

[10] Franz Baader and Wayne Snyder. Unification theory. In John Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning (in 2 volumes)*, pages 445–532. Elsevier and MIT Press, 2001. 2

[11] Mathieu Baudet. Deciding security of protocols against off-line guessing attacks. In Vijay Atluri, Catherine Meadows, and Ari Juels, editors, *Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS 2005, Alexandria, VA, USA, November 7-11, 2005*, pages 16–25. ACM, 2005. 1.1

[12] Mathieu Baudet, Véronique Cortier, and Stéphanie Delaune. YAPA: A generic tool for computing intruder knowledge. *ACM Transactions on Computational Logic*, 14(1):4:1–4:32, February 2013. 1.2, 8

[13] Mathieu Baudet, Bogdan Warinschi, and Martín Abadi. Guessing attacks and the computational soundness of static equivalence. *Journal of Computer Security*, 18(5):909–968, 2010. 1.1

[14] Steven M. Bellovin and Michael Merritt. Limitations of the Kerberos authentication system. In *Proceedings of the Usenix Winter 1991 Conference, Dallas, TX, USA, January 1991*, pages 253–268. USENIX Association, 1991. 1.1

[15] Bruno Blanchet. An efficient cryptographic protocol verifier based on Prolog rules. In *14th IEEE Computer Security Foundations Workshop (CSFW-14 2001), 11-13 June 2001, Cape Breton, Nova Scotia, Canada*, pages 82–96. IEEE Computer Society, 2001. 1.2

[16] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. Trace equivalence decision: negative tests and non-determinism. In Yan Chen, George Danezis, and Vitaly Shmatikov, editors, *Proceedings of the 18th ACM Conference on Computer*

and Communications Security, CCS 2011, Chicago, Illinois, USA, October 17-21, 2011, pages 321–330. ACM, 2011. 1.2

[17] Yannick Chevalier and Michaël Rusinowitch. Compiling and securing cryptographic protocols. *Information Processing Letters*, 110(3):116–122, 2010. 1.1

[18] Bruno Conchinha, David A. Basin, and Carlos Caleiro. Efficient decision procedures for message deducibility and static equivalence. In Pierpaolo Degano, Sandro Etalle, and Joshua D. Guttman, editors, *Formal Aspects of Security and Trust - 7th International Workshop, FAST 2010, Pisa, Italy, September 16-17, 2010. Revised Selected Papers*, volume 6561 of *Lecture Notes in Computer Science*, pages 34–49. Springer, 2010. 1.2

[19] Bruno Conchinha, David A. Basin, and Carlos Caleiro. FAST: an efficient decision procedure for deduction and static equivalence. In Manfred Schmidt-Schauß, editor, *Proceedings of the 22nd International Conference on Rewriting Techniques and Applications, RTA 2011, May 30 - June 1, 2011, Novi Sad, Serbia*, volume 10 of *LIPIcs*, pages 11–20. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2011. 1.2, 8

[20] Bruno Conchinha, David A. Basin, and Carlos Caleiro. Symbolic probabilistic analysis of off-line guessing. In Jason Crampton, Sushil Jajodia, and Keith Mayes, editors, *Computer Security - ESORICS 2013 - 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013. Proceedings*, volume 8134 of *Lecture Notes in Computer Science*, pages 363–380. Springer, 2013. 1.1

[21] Ricardo Corin, Jeroen Doumen, and Sandro Etalle. Analysing password protocol security against off-line dictionary attacks. *Electronic Notes in Theoretical Computer Science*, 121:47–63, 2005. 1.1

[22] Véronique Cortier and Stéphanie Delaune. Deciding knowledge in security protocols for monoidal equational theories. In Nachum Dershowitz and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning, 14th International Conference, LPAR 2007, Yerevan, Armenia, October 15-19, 2007, Proceed-*

ings, volume 4790 of *Lecture Notes in Computer Science*, pages 196–210. Springer, 2007. 1.2

[23] Ştefan Ciobâcă, Stéphanie Delaune, and Steve Kremer. Computing knowledge in security protocols under convergent equational theories. *Journal of Automated Reasoning*, 48(2):219–262, 2012. 1.2, 8

[24] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. 6

[25] Danny Dolev and Andrew C. Yao. On the security of public key protocols. *Information Theory, IEEE Transactions on*, 29(2):198–208, Mar 1983. 1.1

[26] Santiago Escobar, Catherine Meadows, and José Meseguer. Maude-NPA: Cryptographic protocol analysis modulo equational properties. In *Foundations of Security Analysis and Design V, FOSAD 2007/2008/2009 Tutorial Lectures*, volume 5705 of *Lecture Notes in Computer Science*, pages 1–50. Springer, 2009. 8

[27] Donald E. Knuth and Peter B. Bendix. Simple word problems in universal algebras. In Jörg H. Siekmann and Graham Wrightson, editors, *Automation of Reasoning*, Symbolic Computation, pages 342–376. Springer Berlin Heidelberg, 1983. 1.2, 8

[28] T. Mark A. Lomas, Li Gong, Jerome H. Saltzer, and Roger M. Needham. Reducing risks from poorly chosen keys. *ACM Special Interest Group on Operating Systems (SIGOPS) Operating Systems Review*, 23(5):14–18, November 1989. 1.2

[29] Gavin Lowe. Analysing protocols subject to guessing attacks. *Journal of Computer Security*, 12(1):83–98, 2004. 1.1

[30] Jorge Munilla and Alberto Peinado. HB-MP: A further step in the HB-family of lightweight authentication protocols. *Computer Networks*, 51(9):2262–2267, 2007. 1.1

[31] Paliath Narendran. private communication, 2015. 1.2, A

[32] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. 6

[33] Michaël Rusinowitch. private communication, 2015. 1.2, A

[34] Mark D. Ryan and Ben Smyth. Applied pi calculus. In Véronique Cortier and Steve Kremer, editors, *Formal Models and Techniques for Analyzing Security Protocols: A Tutorial*, volume 1 of *Foundations and Trends in Programming Languages*, pages 151–267. 2014. 1.2