message of the form that some honest agent is expecting to receive, or whether he is able to obtain a message that is intended to be a secret, e.g. a key shared by two honest agents.

In this paper, we focus on the intruder deduction problem in the presence of algebraic equations that express properties of cryptographic operators. The underlying intruder model we employ is that of Dolev and Yao [19], in which

cryptography). These bounds control the complexity of the equational unification problems that arise, transforming undecidable problems into decidable ones. Moreover, these bounds effectively serve as search parameters that can be used to control the search over the space of messages.

Our framework is thus parameterized by algebraic theories of the two kinds above and provides a general algorithm for the algebraic intruder deduction problem when the depth of message terms and the analysis operations of the intruder are bounded. Our framework allows us to identify several sub-problems of the intruder deduction problem (e.g. the reduction of terms to their normal forms) and provide general algorithms for them. Along the way, we also show that the problems considered become undecidable when any of the restrictions made in our framework are removed.

Two remarks are in order to help put into context our use of depth parameters. First, rather than considering specialized theories of algebraic properties

symbols of arity n. Terms in Σ^0 are *constants* (i.e. nullary function symbols) and represent *atomic messages* like agent names or nonces. We define the *depth* of a term t as the number of nodes in the longest path from the root to a leaf in its tree representation, and the *size* of t

domain(θ). Given a set S of substitutions, S_0

Definition 2. *Given a finite set of ground terms IK (for "intruder knowledge") and an equational theory E, we define $DY_E(IK)$ (for "Dolev-Yao") as the least set that is closed under the rules*

t_1, t_2 of two messages t_1 and t_2, *modular exponentiation* $exp(t_1, t_2)$ of a message t_1 with a message t_2, and *bitwise xor* $t_1 \quad t_2$ of a message t_1 with a message t_2

We can then, for example, prove that F_{ex} is an FEC theory and C_{ex} is a

Definition 5. *We call a* bounded variable *a variable for which only terms with*

derivations modulo $F \quad C$. In particular, given a set IK of ground terms, we

knows the messages $\{|m|\}_{k_1,k_2}$ and k_1 and k_2, then he can analyze the encrypted message, but only after synthesizing the key k_1,k_2 . We now define a general notion of analysis based on an arbitrary cancellation theory C.

Intuitively, we speak of *synthesis* when the intruder applies the OP rule to compose terms, excluding the case when the resulting composed term is a redex according to the cancellation theory C (as we can then reduce it to a simpler term). We speak of

Theorem 4. *There is an FEC theory F*

the protocol analysis problem, along with other parameters like the number of

15. H. Comon-Lundh and S. Delaune. The finite variant property: How to get rid of some algebraic properties. In *Proc. RTA'05*, LNCS 3467, pp. 294–307. Springer, 2005.

15. H. Comon and V. Shmatikov. Is it possible to decide whether a cryptographic protocol is secure or not? *Journal of Telecommunications and Information Technology*, 4:5–15, 2002.