2014 IEEE 27th Computer Security Foundations Symposium

Modeling Diffie-Hellman Derivability for Automated Analysis

Moses Liskov and F. Javier Thayer

***Abstract*—Automated analysis of protocols involving Diffie-Hellman key exchange is challenging, in part because of the undecidability of the unification problem in relevant theories. In this paper, we justify the use of a more restricted theory that includes multiplication of exponents but not addition, providing unitary and efficient unification.**

To justify this theory, we compare it to a computational model of non-uniform circuit complexity through several incremental steps. First, we give a model closely analogous to the computational model, in which derivability is modeled by closure under simple algebraic transformations. This model retains many of the complex features of the computational model, including defining success based on asymptotic probability for a non-uniform family of strategies. We describe an intermediate model based on formal polynomial manipulations, in which success is exact and there is no longer a parametrized notion of the strategy. Despite the many differences in form, we are able to prove an equivalence between the asymptotic and intermediate models by showing that a sufficiently successful asymptotic strategy implies the existence of a perfect strategy. Finally, we describe a symbolic model in which addition of exponents is not modeled, and prove that (for expressible problems), the symbolic model is equivalent to the intermediate model.

I. Introduction

Automated analysis of protocols involving Diffie-Hellman key exchange [10] is a challenging area that has attracted much recent interest [7], [11], [16], [20]. Diffie-Hellman key exchange differs from other protocol building blocks in that its security properties are more difficult to describe than the underlying derivability assumptions that guarantee those properties. Thus, it is typical to focus on modeling derivability in Diffie-Hellman environments.

Much of this work deals with a restricted theory of Diffie-Hellman derivability that includes multiplication of exponents but not addition. This paper focuses on the problem of giving a rigorous justification for formal modeling of Diffie-Hellman derivability, especially including this restricted view. Our approach to justification is to compare our model to a computational model for derivability in the Diffie-Hellman scenario. The computational model we work with is computability by a polynomially bounded non-uniform family of randomized circuits with non-negligible probability.

In comparing the computational model, the validity of which is well accepted, to this restricted DH theory, we observe a number of major differences. First, the computational model is parametrized and deals with non-uniform families of circuits that represent strategies. The symbolic theory is not parametrized and aims to capture only generic solutions. The computational model is based on probability and incorporates randomness both in the challenge to be solved and in the circuits that attempt to solve it. There is no notion of probability in the symbolic theory: derivability is an all-or-nothing proposition. Finally, the notion of derivations in the symbolic theory is based on closure under simple, obviously-computable algebraic transformations, while the computational model gives a more implicit definition of what is computable. The last of these does represent a fundamental difference in the models, but we establish in this paper that the *other* differences are not fundamental.

We justify the restricted model as follows. First, we give a model closely analogous to the computational model, in which derivability is modeled by closure under simple algebraic transformations. The gap between this model and the computational one is unknown, but such a change in our notion of derivability is necessary to make at some point. Moreover, considering this model is a *minimal* change of this type, since this model retains all complex features of the computational model, including defining success based on asymptotic probability for a non-uniform family of strategies. Second, we describe a rich Diffie-Hellman theory modeling both multiplication and addition of exponents, but with an exact notion of derivability not involving asymptotic behavior or probability. We prove that derivability in the asymptotic model is equivalent to derivability in this intermediate model. Then we present the symbolic restricted model in which addition of exponents is not modeled, and prove that, for derivability problems expressible without reference to addition of exponents, derivability in the restricted model is equivalent to derivability in the intermediate model.

Non-standard analysis.

The problem of dealing with the asymptotic behavior of a parameterized sequence of objects is similar to a long-standing problem with calculus. The concept of an infinitesimal number, greater than zero but smaller than all positive numbers, does not fit comfortably with theories of the real numbers. Therefore the standard approach to calculus deals with sequences and limits. There is, however, another approach to this problem, to enhance our notion of numbers in such a way that infinitesimals can be rigorously justified: non-standard analysis.

In non-standard analysis, we may view sequences parameterized by the integers as extensible to non-standard integers, including hyperfinite ones. When we extend the sequence of Diffie-Hellman parameters to a hyperfinite index, we obtain a field of hyperfinite prime order. Dougherty and Guttman have described a model for Diffie-Hellman as an ultraproduct

DOI 10.1109/CSF.2014.24

[11], which is effectively identical. However, the use of ultraproducts soon becomes burdensome for the other objects; our use of non-standard analysis allows us to apply the same approach to notions of probability, nonuniform families of circuits, and so on. Most particularly, we are able to describe the notions of negligible and non-negligible probability via measure at a hyperfinite index.

The results we obtain in the nonstandard setting imply completely standard results about families of computational problems indexed by a security parameter. That this transition from nonstandard to standard is valid follows from the transfer principle and the known theorem that nonstandard analysis is a conservative extension of ZFC set theory. In fact [18] gives an algorithm to "unwind" any proof of a standard result using nonstandard methods to a standard one. However, the nonstandard formulation provides an intuitively appealing framework for proving asymptotic security properties.

All-or-nothing nature of polynomial derivations.

Our model of Diffie-Hellman derivability is based on polynomial[1] derivation. Although we define the success of polynomial derivation probabilistically (over uniform choices of unknown exponents), and although we allow a non-uniform family of polynomials restricted only by a very generous limitation on degree, it turns out this is no more descriptive than a single uniform polynomial that exactly matches the target. This is a consequence of the fact that polynomials that have more zeroes than their degree over a finite field must be uniformly zero.

Conservative extension.

Once we have justified the rich polynomial-derivation model, the remaining issue is how to justify our restricted model, in which derivability is based on monomials rather than polynomials. Such a restriction necessarily reduces the set of derivability problems we can describe, but the justification issue remains: since we know all polynomial derivations are feasible, are we making too bold a restriction on the power of the adversary?

We answer this question in the negative. We prove that any monomial that can be expressed as a polynomial of monomials can be expressed as a monomial of those same monomials, and use this to prove that any polynomial-derivable problem that can be expressed in the restricted model is monomial-derivable. In other words, we are restricting our scope but not fundamentally changing the derivability of any statements by restricting the model.

A. Prior work

Diffie-Hellman models.

Automated analysis of security protocols has received much attention in recent years. Early work on such techniques focused on modeling basic building blocks of secure protocols such as encryption [1], [5], [19], but researchers have more and more turned their attention to capturing the implicit security properties of algebraic structures such as those that drive the Diffie-Hellman protocol [10].

Symbolic modeling is the primary approach to accomplishing automated analysis. There has been substantial work on modeling DH key agreement. Boreale and Buscemi [6] and Goubault-Larrecq, Roger, and Verma [14] describe symbolic reasoning approaches for DH. Tools such as Maude-NPA [12] and Tamarin [20] incorporate symbolic reasoning into automated analysis of protocols involving DH. All of these works have two features in common: they rely on solving unification problems as a core functionality in their analysis, and they model only the multiplication of exponents but do not model their addition.

Dougherty and Guttman present an algebraic framework for DH that does model addition of exponents [11]. They note that this is challenging partly because unification is undecidable in the theory of rings, by the unsolvability of Hilbert's tenth problem. There are, however, other related theories that are decidable [15], [16]. Thus, while our restricted model is not *universally* relied upon in prior work on symbolic analysis of DH protocols, it is the norm.

On comparing computational and symbolic approaches.

Although symbolic security analysis has had numerous successes, a recurrent theme in criticism of such work is that it relies on models that are too abstract, and that not enough is understood about the implications of adopting such models. Much research in the cryptologic community is based on a far less abstracted model of computational hardness that traces its roots to work of Goldwasser and Micali [13]. Symbolic approaches are not alone in being the target of such criticism: wherever work in the cryptologic community involves highly abstracted elements such as the random oracle model of Bellare and Rogaway [4] or Shoup's generic group model [21], their use is regarded as an undesirable feature.

Although the computational model and symbolic models remain far apart, there have been some important contributions in understanding the relationship between them. The most important class of results is the approach known as *computational soundness*, in which the aim is to identify the requirements for security proofs in symbolic models to hold in a computational one [1], [3], [9], [17]. The computational soundness approach has also been applied to a symbolic model capturing DH keys by Bresson et al [7].

Our paper presents a different type of result. We aim to show that a practically useful symbolic model is equivalent to a well-accepted computational model, under an assumption that would clearly be necessary to conclude such a result.

B. Structure of the paper

In Section II we cover basic background material and define the notion of a Diffie-Hellman derivation problem. In Section III we describe four derivability models for Diffie-Hellman problems: the computational model, the asymptotic

[1] "Polynomial" here is a handy description but not fully accurate. Actually the adversary can compute any rational function (quotient of polynomials) on exponents and can raise any known base to any derivable exponent. Similarly we use "monomial" derivation as a name for our restricted model, but again the adversary may also involve bases.

polynomial model, the formal polynomial model, and the monomial model, the last of which is the symbolic model we seek to justify. We then state the main theorems of the paper. In Section IV, we give an exposition of the concepts of non-standard analysis and discuss how these concepts may apply to asymptotic models. In Section V, we address the proof of the first main theorem: the equivalence of the asymptotic polynomial model and the formal polynomial model. In Section VI, we prove the second main theorem: the equivalence of derivability in the formal polynomial and monomial models, for monomial derivation problems.

II. Diffie-Hellman derivation problems

The Diffie-Hellman protocol is described in a finite group G of prime order $\mathrm{Ord}(G) = p$, along with a generator g. It is believed that in such groups the "discrete logarithm problem" of finding a random x given (G, g, g^x) is hard. It is further believed that if x and y are random, it is hard to find g^{xy} given (G, g, g^x, g^y); this is called the computational Diffie-Hellman problem.

The hardness of these computational problems is the basis of Diffie-Hellman key exchange and many other cryptographic techniques. There are certain aspects of the standard computational model in which statements of the tractability or intractability of such problems are stated that need to be reviewed here. In particular, it is important to state the computational hardness of such problems in a way that seems realistic.

First of all, such statements are asymptotic ones. These problems may be solved via brute force if the prime order p is small enough. Thus, any asymptotic definition will necessarily include an infinite family of p, G, and g. However, one attractive feature of discrete logarithm-based cryptography is that no "trap-door" is thought to exist making the discrete logarithm problem or the computational Diffie-Hellman problem easy under a given set of parameters. Thus, the same parameters can be used by everyone.

Second, hardness is meant to be as close as possible to impossibility, but we must recognize that randomized algorithms will always be able to have a tiny chance of success, for instance, by guessing the right answer at random. Thus, the standard computational model concerns problems that can be solved with non-negligible probability.

A. Preliminaries and notation

The expression $\Pr[v_1 \leftarrow A_1; \ldots; v_n \leftarrow A_n : P(v_1, \ldots, v_n)]$ denotes the probability that $P(v_1, \ldots, v_n)$ holds given assignment of each of v_1 through v_n based on probability distributions $A_1, \ldots, A_n$. When a finite set is given in place of a probability distribution, the uniform distribution on that set is implied. When an algorithm is in place of a probability distribution, it is implied that a run of that algorithm is performed, with uniform randomness if the algorithm is randomized.

Negligible functions. A function $f : \mathbb{N} \longrightarrow \mathbb{R}$ is *negligible* if and only if for every positive n there is a positive constant C such that $|f(k)| \leq Ck^{-n}$. This is equivalent to the form preferred in the cryptography literature:

$$\forall n \in \mathbb{N}\ \exists k_0\ \forall k \geq k_0\ |f(k)| \leq k^{-n} \tag{1}$$

Condition (1) clearly implies negligibility. Conversely, if f is negligible, for positive n there is a C such that $|f(k)| \leq Ck^{-(n+1)}$ for all k. Let k_0 be such that $Ck_0^{-1} \leq 1$. Then $|f(k)| \leq k^{-n}$. Contrapositively, a function is f *non-negligible* if and only if there are n and infinitely many k such that $|f(k)| \geq k^{-n}$.

A *rational expression with integer coefficients* is an element of the field of quotients of the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$. We denote it by $\mathbb{Z}(x_1, \ldots, x_n)$. A *monomial* is an expression of the form $M(\bar{x}) = \bar{x}^{\bar{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ where $n \in \mathbb{N}$ and $\alpha_i \in \mathbb{Z}$. We associate to the monomial M the function (which by abuse of language we also denote by M) $\bar{a} \mapsto a_1^{\alpha_1} \cdots a_n^{\alpha_n}$ defined whenever all $a_i \neq 0$.

We use a bar to indicate a sequence of values. Thus, we may describe a particular rational expression as $R(\bar{x})$, which leaves ambiguous the value of n such that $R \in \mathbb{Z}(x_1, \ldots, x_n)$. If $\bar{R}$ is a sequence of rational expressions $\bar{R} = R_1, \ldots, R_n$, we can use $\bar{R}(\bar{x})$ to refer to $(R_1(\bar{x}), \ldots, R_n(\bar{x}))$ and $g^{\bar{R}(\bar{x})}$ to refer to $(g^{R_1(\bar{x})}, \ldots, g^{R_n(\bar{x})})$.

Systems of exponent environments. Let G be a cyclic group of prime order p. Since G is of prime order, every $g \in G$ such that $g \neq 1_G$ is a generator for G. In particular, exponentiation is a mapping $G \times \mathbb{Z} \to G$. However, since g^k depends only on the equivalence class of k modulo p, we can view exponentiation as a mapping $G \times \mathbb{Z}/(p) \to G$. We thus view the set of exponents as a field. Suppose G_k is a sequence of such cyclic groups where each G_k is of prime order p_k, such that $p_k \to \infty$. Assume that g_k is a sequence of generators for each G_k.

Definition 1: A sequence $\mathcal{S} = \{(G_k, g_k, p_k) : k \in \mathbb{N}\}$ is an *admissible system of exponentiation environments* if G_k is a cyclic group of prime order p_k, where g_k is a generator, and there are constants $0 < c \leq C < \infty$ and $0 < R < \infty$ such that $c\ R^k \leq p_k \leq C\ R^k$.

Remark 2: It is clear that the exponential growth assumption on p_k is equivalent to the inequality

$$M \log p_k - a \leq k \leq M \log p_k - A \tag{2}$$

for some constants a, A and $M > 0$.

In this paper we are concerned with whether certain values can be derived from certain other values. We restrict to a class of such problems in which the information provided and the values to be derived are both based on rational expressions in the exponent.

Definition 3: A *rational algebraic expression* on variables $x_1, \ldots, x_n$ is either (1) a rational expression $R \in \mathbb{Z}(x_1, \ldots, x_n)$, or (2) g^R where $R \in \mathbb{Z}(x_1, \ldots, x_n)$. If R is a rational algebraic expression we use $R[\bar{x}]$ to denote the value taken by R when $\bar{x}$ is the input to the rational expression within R.

Definition 4: Given an admissible system $\mathcal{S}$ of exponentiation environments, a *derivation problem* for $\mathcal{S}$ is a pair $(\bar{R}_1, R_2)$ where R_2 and the components of $\bar{R}_1$ are rational algebraic expressions.

The derivation problem $(\bar{R}_1, R_2)$ represents the problem of deriving $R_2[\bar{x}]$ from $\bar{R}_1[\bar{x}]$ for random $\bar{x}$.

Note that this notion of a derivation problem includes both presumed hard problems such as the discrete logarithm problem ($\bar{R}_1[x] = g^x$ and $R_2[x] = x$) and the Diffie-Hellman problem ($\bar{R}_1[x_1, x_2] = (g^{x_1}, g^{x_2})$ and $R_2[x_1, x_2] = g^{x_1 x_2}$), but also includes easy problems such as modular exponentiation ($\bar{R}_1[x] = x, R_2[x] = g^x$).

III. Diffie-Hellman Derivability Models

In this section, we describe four models of computation that lead to four distinct notions of solvability for DH derivability problems. Each model has its own notion of acceptable computation strategies as well as a threshold for success. A derivation problem is solvable if there is an acceptable computation strategy that meets the success threshold.

Each notion of solvable gives us a natural corresponding notion of "hard": namely, a derivability problem is hard if it is not solvable.

- The **computational model** involves polynomially bounded non-uniform randomized circuit families, and a family is regarded as successful if it computes the correct result with non-negligible probability.
- The **asymptotic polynomial model** involves non-uniform families of random distributions on log-sublinear-degree polynomial derivations, again with non-negligible probability of success.
- The **formal polynomial model** concerns DH derivation problems in the abstract. A strategy is a polynomial derivation, and success means that the strategy equals the target as algebraic expressions over formal polynomials.
- The **monomial model** is just the same as the formal polynomial model, but strategies are restricted to polynomial derivations which are monomials.

A. The computational model

In order to define the computational view of when a derivation problem is solvable, we must introduce the notion of a polynomially bounded non-uniform randomized circuit family. Roughly, a circuit is a composition of a finite number of NAND gates. The size of a circuit is the number of NAND gates. Each circuit is the implementation of a unique function $\{0,1\}^l \to \{0,1\}^{l'}$.

A randomized circuit is a circuit with a subset of its input bits designated to be random; the non-designated bits are the actual input of the randomized circuit.

A set $\{A_k | k \in \mathbb{N}\}$ of circuits is a non-uniform circuit family. A non-uniform circuit family $\{A_k\}$ is *polynomially bounded* if there exists a polynomial $\rho(k)$ such that for all k, $|A_k| \leq \rho(k)$. Let $\mathcal{PNC}$ be the set of polynomially bounded non-uniform circuit families.

Computation by randomized polynomially-bounded non-uniform circuit families is the most general standard notion for security of discrete logarithm-based cryptographic schemes [8]. The non-uniform stipulation is important to model security where parameters are reused as they often are for Diffie-Hellman. This scenario is a bit more complex than the more typical case of computation by a probabilistic polynomial-time Turing machine, because that amounts to a *uniform* family of circuits rather than a non-uniform one. The distinction is important: computation by a non-uniform family is possible if "trapdoors" exist, whereas computation by a uniform family with those trapdoors would imply that they are efficiently computable.

It is essential to consider the non-uniform case to capture the assumption that there do not exist trapdoors for the common parameters.

Definition 5: A derivation problem $(\bar{R}_1, R_2)$ is *circuit-solvable* if: $\exists\{A_k\} \in \mathcal{PNC} : \Pr[\bar{x} \leftarrow (\mathbb{Z}/(p_k))^n;\ v \leftarrow A_k(\bar{R}_1(\bar{x})) : v = R_2(\bar{x})]$ is non-negligible.

B. Formal strategies

The other three models of derivation involve a formal notion of strategy that corresponds to natural closure rules for the adversary. First we describe these closure rules, and then give a definition of algebraic strategies based on rational functions.

Definition 6 (Closure rules): If U is a set of base values known to the adversary and E is a set of exponents known to the adversary, we expect U and E to be closed under the following rules:

1) $g \in U$ and $0, 1 \in E$.
2) If $u, v \in U$ then $u \cdot v \in U$.
3) If $t_1, t_2 \in E$ then $t_1 t_2 \in E$ and $t_1 + t_2 \in E$.
4) If $0 \neq t \in E$ then $t^{-1} \in E$.
5) If $t \in E$ then $-t \in E$.
6) If $u \in U$ and $t \in E$, then $u^t \in U$.

We next define an algebraic strategy as a way of describing particular implications of these closure rules.

Proposition 7: If E satisfies the closure rules of Definition 6, and if $R \in \mathbb{Z}(x_1, \ldots, x_n)$ and $t_1, \ldots, t_n \in E$ then $R(\bar{t}) \in E$.

Proof: Scalar multiplication of t values can be accomplished by repeated application of Rule 3 and Rule 5 if necessary. Constants are available due to Rule 1. Coefficient-1 monomials may be formed by Rule 3, and thus polynomials may be formed by Rule 3. Rule 4 allows us to form arbitrary rational functions. ∎

Proposition 8: If U and E satisfy the closure rules of Definition 6, and if $R_1, \ldots, R_m \in \mathbb{Z}(x_1, \ldots, x_n)$ and $t_1, \ldots, t_n \in E$ and $u_1, \ldots, u_m \in U$, then $\prod_{i=1}^m {u_i}^{R_i(\bar{t})} \in U$.

Proof: We know each $R_i(\bar{t}) \in E$ due to Proposition 7. Each $u_i^{R_i(\bar{t})}$ is thus in U due to Rule 6, and so $\prod_{i=1}^m {u_i}^{R_i(\bar{t})} \in U$ by Rule 2. ∎

Definition 9: An *algebraic strategy* over exponent variables $\mathbf{E}$ and base variables $\mathbf{U}$ is either (1) a rational expression $R \in \mathbb{Z}(\mathbf{E})$, or (2) a monomial of the form $\prod_{u_i \in \mathbf{U}} {u_i}^{R_i}$ where each $R_i \in \mathbb{Z}(\mathbf{E})$.

Note that due to the closure rules of Definition 6, all derivations have an algebraic strategy.

If $\mathbf{E}$ is a set of exponent variables and $\mathbf{U}$ is a set of base variables, we use $\mathrm{B}\langle \mathbf{U}, \mathbf{E} \rangle$ to denote the set of monomials forming the latter type of algebraic strategy.

An algebraic strategy thus represents an allowable derivation under the closure rules of Definition 6.

If F is an algebraic strategy, and $\bar{h}$ and $\bar{t}$ are tuples of base and exponent values, respectively, we write $F(\bar{h}, \bar{t})$ to indicate the value of F on those inputs: either $R(\bar{t})$ or $\prod_i h_i^{R_i(\bar{t})}$.

C. The asymptotic polynomial model

The asymptotic polynomial model is meant to be a direct analogue of the computational model, but with circuits replaced with algebraic strategies in a direct manner. Instead of non-uniform families of circuits, we deal with non-uniform families of algebraic strategies.

Rather than a polynomial bound on the circuit family, we require that the rational expressions involved are of *log-sublinear* degree in p: in other words, the expressions are of degree significantly less than p. A function $f : \mathbb{R} \longrightarrow \mathbb{R}$ is *log-sublinear* in r if and only if for every $k \in \mathbb{N}$,

$$\lim_{r \to \infty} \frac{f(r)}{r(\log r)^{-k}} = 0. \tag{3}$$

For example, any function such that $f(r) = O(r^{1-\varepsilon})$ for positive ε is log-sublinear. This is a very conservative restriction, because the degree of the rational expressions can still grow exponentially in ℓ, when r has an exponential bound in ℓ. This is the case, for instance, if r is a parameter whose bit length is bounded by ℓ.

Let $\mathcal{LSS}$ (for "log-sublinear strategies") denote the set of non-uniform families of algebraic strategies, such that there is a log-sublinear bounding function f such that the rational expressions in F_k have degree bounded by $f(k)$.

As this model is our "bridge" between the computational and the formal polynomial model, we also refer to this model as our bridge model.

Definition 10: A derivation problem $(\bar{R}_1, R_2)$ is *bridge-solvable* if $\exists \{F_k\} \in \mathcal{LSS} : \Pr[\bar{x} \leftarrow (\mathbb{Z}/(p_k))^n; \bar{y} \leftarrow (\mathbb{Z}/(p_k))^{n'} : R_2(\bar{x}) = F_k(\bar{R}_1(\bar{x})||\bar{y})]$ is non-negligible.

In the definition, $\bar{y}$ is an explicit representation of randomness in the strategy. By $\bar{R}_1(\bar{x})||\bar{y}$ we mean the pair $\bar{h}, \bar{t}||\bar{y}$ where $\bar{R}_1(\bar{x}) = (\bar{h}, \bar{t})$.

D. The formal polynomial model

The formal polynomial model is a much simplified model in which computation strategies are simply single algebraic strategies. The notion of success is equality of formal polynomials (or, more accurately, formal rational expressions). In other words, variables are treated as abstract field extension elements with no non-trivial relations among them.

Definition 11: A derivation problem $(\bar{R}_1, R_2)$ is *formally solvable* if $\exists$ an algebraic strategy $\bar{F}$ such that $R_2 = \bar{F} \circ \bar{R}_1$.

This allows us to state the first main theorem of the paper.

Theorem 12: Derivation problems are formally solvable if and only if they are bridge-solvable.

Sorts:	BASE, EXPN
$(\cdot)^{(\cdot)}$	BASE $\times$ EXPN $\rightarrow$ BASE
$\cdot\,\cdot$	EXPN $\times$ EXPN $\rightarrow$ EXPN
$(\cdot)^{-1}$	EXPN $\rightarrow$ EXPN
1	EXPN
g	BASE

Equations

$g^{xy} \equiv (g^x)^y$	g: BASE, x, y: EXPN
$xy \equiv yx$	x, y: EXPN
$x(yz) \equiv (xy)z$	x, y, z: EXPN
$g^1 \equiv g$	g: BASE
$1x \equiv x$	x: EXPN
$x(x^{-1}) \equiv 1$	x: EXPN

Derivations

$\emptyset \vdash g, 1$	
$x, y \vdash xy$	x, y: EXPN
$x \vdash x^{-1}$	x: EXPN
$h, x \vdash h^x$	h: BASE, x: EXPN

Fig. 1. Our restricted Diffie-Hellman algebra

E. The monomial model

Unfortunately, the formal polynomial model is not a symbolic model. Prior work on automated protocol analysis focuses on symbolic models in which the addition of exponents is not represented [6], [12], [14], [20]. Moreover, Dougherty and Guttman observe that the notion that all exponents other than 0 have inverses cannot be simply expressed in an equational theory [11], so it may be necessary to make such a restriction in order to have a symbolic model for DH derivability.

Definition 13: An algebraic strategy is *monomial* if all the rational expressions involved are monomials.

Definition 14: A derivation problem $(\bar{R}_1, R_2)$ is *monomial solvable* if $\exists$ a monomial algebraic strategy $\bar{F}$ such that $R_2 = \bar{F} \circ \bar{R}_1$

For *monomial* derivation problems $(\bar{R}_1, R_2)$ (those involving only monomials), monomial solvability is equivalent to derivability in the Diffie-Hellman algebra and derivability model illustrated in Figure 1. The derivability rules are simply those of Definition 6 restricted to the multiplicative rules for exponents.

This brings us to the statement of our second main theorem:

Theorem 15: For all monomial derivability problems $(\bar{R}_1, R_2)$, $(\bar{R}_1, R_2)$ is monomial solvable if and only if it is formally solvable.

IV. Non-standard Analysis

Our next aim is to prove the main theorems of the paper, starting with the proof of Theorem 12.

In order to prove equivalence of bridge and formal solvability, we apply ideas from non-standard analysis to the asymptotic polynomial model. Specifically, we consider that asymptotic definition at an appropriate infinite index. Bridge solvability is thus equivalent to a non-negligibly successful

$\mho$	${}^\circ\mho$	$\mho$	${}^\circ\mho$
$\in$	$\in$	$\mathbb{N}$	${}^\bullet\mathbb{N}$
$\subseteq$	$\subseteq$	$\mathbb{R}$	${}^\bullet\mathbb{R}$
$\bigcup$	$\bigcup$	$\sum$	${}^\bullet\sum$
$(\cdot,\cdot)$	$(\cdot,\cdot)$	$\prod$	${}^\bullet\prod$
$\mathcal{P}$	${}^\bullet\mathcal{P}$	function	function
card	${}^\bullet$card	finite	${}^\bullet$finite

TABLE I
TRANSLATION TABLE FOR RELATIONS, OPERATORS AND PREDICATES

solution by a non-uniform family of randomized strategies. We show this implies the existence of some uniformly successful strategy via an argument about the size of non-trivial algebraic varieties.

In this section, we give a basic exposition of non-standard analysis and describe the main technique of choosing an infinite index, and how this applies to concepts such as probability and negligible functions. In the next section, we prove the first main theorem.

A. Basic concepts of non-standard analysis

Beyond its foundational role for a theory of infinitesimals, non-standard analysis provides a general and efficient limit construction for sequences of discrete objects [22]. Our reference for non-standard analysis is [2]. The main constituents of non-standard analysis are a pair of universes $\mho$ and ${}^\circ\mho$ and an operator ${}^\bullet : \mho \longrightarrow {}^\circ\mho$ called an *enlargement operator*. The *transfer principle* is the fact that the operator ${}^\bullet$ preserves the validity of first order formulas. Mathematical terms such as function, cardinality, finiteness, field can be carried over to ${}^\circ\mho$ and the enlargement operator preserves their basic properties. We will refer to $\mho$ as the *standard universe* and ${}^\circ\mho$ as the *non-standard universe*. The transfer principle is stated as follows:

Axiom 16 (Transfer): If $\Phi(x_1,\ldots,x_n)$ is a formula with bounded quantification whose free variables are among $x_1,\ldots,x_n$, then for $a_1,\ldots,a_n \in \mho$, $\Phi(a_1,\ldots,a_n)$ is valid in $\mho$ if and only if $\Phi({}^\bullet a_1,\ldots,{}^\bullet a_n)$ is valid in ${}^\circ\mho$.

By formula we mean first order formula with the predicate symbols "$\in$" and "$=$" and some constants such as 1 and $\mathbb{N}$. The restriction to bounded formulas is not strictly necessary, but it allows us to assume that the model ${}^\circ\mho$ interprets the membership operator as $\in$. The reference [2] follows this approach while [18] allows for unrestricted quantifiers.

We could build a correspondence table between symbols in the standard universe and symbols in the non-standard one. To each construct (predicate, operator, relation) C in the standard universe corresponds a construct ${}^\bullet C$ in the non-standard universe. The table would look something like the table in Figure I. The notations that are used in practice differ from those in this list. For example, for the predicates ${}^\bullet$finite, ${}^\bullet$integer, ${}^\bullet$real we use *hyperfinite, hyperinteger, hyperreal* respectively, A partial mapping $\varphi : {}^\circ\mho \longrightarrow {}^\circ\mho$ is *internal* if there is an $f \in {}^\circ\mho$ satisfying the function predicate such that $\varphi(a)$ is defined if and only if $a \in {}^\bullet\mathrm{dom} f$ and for such values of a, $\varphi(a) = f(a)$. Otherwise, the mapping is said to be *external*. A set is internal (respectively external) if and only if its indicator function is internal (respectively external).

Elements r of a set S are identified with ${}^\bullet r$. Thus S is viewed as a subset of ${}^\bullet S$.

An element $u \in {}^\circ\mho$ is *standard* if and only if $u = {}^\bullet x$ for some $x \in \mho$. Thus ${}^\bullet\mathbb{N}$ and ${}^\bullet\mathbb{R}$ are standard sets *even though they have non-standard elements*. We denote the formula "x is standard" by $\mathrm{st}(x)$. We use the notation $\forall^{\mathrm{st}} x \Phi(x)$ and $\exists^{\mathrm{st}} x \Phi(x)$ which are abbreviations for the formulas $\forall x\ [\mathrm{st}(x) \implies \Phi(x)]$ and $\exists x\ [\mathrm{st}(x) \wedge \Phi(x)]$ respectively. More generally, if Φ is a first order formula, Φ^{st} is the formula where all quantifications of the form $\forall x$ and $\exists x$ are replaced with quantifications $\forall^{\mathrm{st}} x$ and $\exists^{\mathrm{st}} x$ respectively. The transfer principle then takes the form:

Axiom 17: If $\Phi(x_1,\ldots,x_n)$ is a bounded formula whose free variables are among $x_1,\ldots,x_n$, then for all standard $a_1,\ldots,a_n \in {}^\circ\mho$,

$$\Phi^{\mathrm{st}}(a_1,\ldots,a_n) \iff \Phi(a_1,\ldots,a_n).$$

Non-standard analysis uses, in an essential way, the non-standard integers. The following principle guarantees their existence:

Axiom 18 (Countable Saturation): If $\{A_n : n \in \mathbb{N}\}$ is a sequence of internal sets in ${}^\circ\mho$ such that for all $n \in \mathbb{N}$ $A_1 \cap A_2 \cap \cdots \cap A_n$ is non-empty, then there is an internal element a such that $a \in A_n$ for all $n \in \mathbb{N}$.

Proposition 19: ${}^\bullet\mathbb{N} \setminus \mathbb{N}$ is non-empty.

Proof:

For finite subsets of $\mho$ we have

$${}^\bullet\{a_1,\ldots,a_n\} = \{{}^\bullet a_1,\ldots,{}^\bullet a_n\}. \tag{4}$$

Now $\mathbb{N} \setminus \{1,\ldots,n\}$ is non-empty. Therefore for all $n \in \mathbb{N}$,

$$A_n = {}^\bullet\mathbb{N} \setminus \{1,\ldots,n\} \neq \emptyset$$

and thus there is an $a \in \bigcap_k A_k$. Such an a is distinct from all $k \in \mathbb{N}$. ∎

Countable saturation also establishes the following principle:

Proposition 20 (Extension of sequences principle.): For any sequence $\{a_n\}_{n\in\mathbb{N}}$ of elements of ${}^\circ\mho$ such that $a_n \in A$, there is an internal sequence $\{a'_n\}_{n\in{}^\bullet\mathbb{N}}$ which extends the original sequence, that is $a'_n = a_n$ for all $n \in \mathbb{N}$.

Proof: For each $n \in \mathbb{N}$, let A_n be the set of sequences $\{b_k\}_{k\in{}^\bullet\mathbb{N}}$ which coincide with $\{a_k\}_{k\in\mathbb{N}}$ in the interval $\{1,2,\ldots,n\}$. For all $n \in \mathbb{N}$, A_n is non-empty since we can exhibit an element $b \in A_n$ as follows:

$$b_k = \begin{cases} a_k & \text{if } k \leq n \\ 0 & \text{otherwise} \end{cases}$$

The sequence is internal, since it is defined by an internal formula. By countable saturation, there is an internal a that is an element of all the sets A_n. ∎

Some interesting non-standard numbers we can create using this principle include *infinitesimal* numbers and *infinite* numbers.

Definition 21: An $r \in {}^\bullet\mathbb{R}$ is *infinitesimal* if and only if for every $n \in \mathbb{N}$, $|r| \leq n^{-1}$.

x is infinitesimal is written as $x \simeq 0$.

Proposition 22: There are infinitesimal hyperreal numbers.

Proof: For $n \in \mathbb{N}$, let $A_n = \{r \in {}^\bullet\mathbb{R} : 0 \leq r \leq 1/n\}$. A_n is non-empty and this by countable saturation, $\bigcap_n A_n$ is non-empty. ∎

Definition 23: A positive hyperreal r is *infinite*, written as $x \simeq \infty$, if and only if $\forall n \in \mathbb{N}$, $r \geq n$.

We use the notation $r \gg 0$ to indicate r is not infinitesimal and $r \ll \infty$ to indicate r is not infinite.

Besides the ubiquitous transfer principle, we use two other techniques of non-standard analysis: *countable saturation* in the form of the extension of sequences principle and the *overspill principle* according to which any internal property which holds for all elements of a non-internal set must spill over into at least one non-standard element.

B. Non-standard treatment of asymptotic derivability models

Remark 24 (Notation): Given any standard sequence $\mathcal{S} = \{S_k\}_{k\in\mathbb{N}}$, ${}^\bullet\mathcal{S}$ denotes the family indexed by ${}^\bullet\mathbb{N}$ obtained by applying the transfer operator to $\mathcal{S}$. The family ${}^\bullet\mathcal{S}$ can be viewed as extension of $\mathcal{S}$. By overloading of notation, we denote each term of the family ${}^\bullet\mathcal{S}$ by S_k.

Now let $\mathcal{S} = \{(G_j, g_j, p_j) : j \in \mathbb{N}\}$ be an admissible system of groups and generators; ${}^\bullet\mathcal{S}$ is a family indexed on ${}^\bullet\mathbb{N}$ which extends $\mathcal{S}$. By transfer, for each $k \in {}^\bullet\mathbb{N}$, G_k is a cyclic group, generated by g_k, of prime order p_k. In particular, exponentiation is defined as a mapping $G_k \times \mathbb{Z}/(p_k) \to G_k$. Now let $k \simeq \infty$. Then $p_k \simeq \infty$ due to growth requirements on the sequence $\{p_k\}_k$ in Definition 1. The internal characteristic of this field is $p_k \simeq \infty$.

Non-standard view of negligibility

First, we prove the following proposition.

Proposition 25: A necessary and sufficient condition for a (standard) function f on $\mathbb{N}$ to be negligible is that for all standard n and $k \simeq \infty$, $|{}^\bullet f(k)| \leq k^{-n}$.

Proof: For necessity, suppose f is negligible and n is standard. By the definition of negligible

$$\exists^{\mathrm{st}}\ell\ \forall^{\mathrm{st}}k \geq \ell\ |{}^\bullet f(k)| \leq k^{-n}$$

is valid. Applying transfer, which is legitimate since it is applied to the innermost quantifier

$$\exists^{\mathrm{st}}\ell\ \forall k \geq \ell\ |{}^\bullet f(k)| \leq k^{-n}$$

In particular, if $k \simeq \infty$, $|{}^\bullet f(k)| \leq k^{-n}$ as claimed.

The proof of sufficiency relies on a common technique involving overspill and transfer. Suppose that for all $k \simeq \infty$ and all standard n, $|{}^\bullet f(k)| \geq k^{-n}$. In particular,

$$\forall \ell \simeq \infty\ \forall k \geq \ell\ |{}^\bullet f(k)| \geq k^{-n}$$

and thus by overspill,

$$\exists^{\mathrm{st}}\ell\ \forall k \geq \ell\ |{}^\bullet f(k)| \geq k^{-n}$$

By transfer

$$\exists^{\mathrm{st}}\ell\ \forall^{\mathrm{st}}k \geq \ell\ |{}^\bullet f(k)| \geq k^{-n}$$

which is the claim f is negligible. ∎

Non-standard view of probability

Let $\mathcal{X} = \{X_k\}_{k\in\mathbb{N}}$ be a sequence of finite sets. A sequence of subsets $A_k \subseteq X_k$ is *negligible* if and only if $\Pr_k(A_k)$ is negligible as a function of k, where $\Pr_k$ is the uniform probability measure on X_k.

We will consider any hyperfinite set X as a space equipped with the probability measure

$$\Pr(A) = \frac{{}^\bullet\mathrm{card}\, A}{{}^\bullet\mathrm{card}\, X} \tag{5}$$

Proposition 26: Let $\{X_k\}_{k\in\mathbb{N}}$ be a sequence of finite sets. A necessary and sufficient condition a sequence $\{A_k\}_k$ of subsets be negligible is that for every standard m and $k \simeq \infty$

$$\Pr(A_k) \leq k^{-m} \tag{6}$$

Proof: The proof of this follows the same lines as the proof of Proposition 25. ∎

Definition 27: Let $K \simeq \infty$. A hyperreal θ is K-negligible if and only if for all standard m, $|\theta| \leq K^{-m}$. A hyperreal θ is of order K if and only if there is a standard m, such that $|\theta| \leq K^{-m}$.

Remark 28: Any K-negligible number θ is infinitesimal, since $\theta \leq K^{-1}$ and K^{-1} is already infinitesimal. The converse is false, since K^{-1} is infinitesimal but not negligible. We introduce this stronger concept motivated by Proposition 26 and the transfer principle to translate the property of negligible sequence into a "limit" property of a single hyperfinite set. Note that negligible is defined relative to a scale parameter K.

In the statement of Proposition 26 there is no relation assumed between the cardinality of X_k and k. If we assume X_k has an exponential growth, that is for some constants $0 < c \leq C < \infty$ and all k,

$$c \leq \frac{\mathrm{card}\, X_k}{R^k} \leq C$$

then we can rewrite (6) as for all $k \simeq \infty$, $\Pr_k(A_k)$ is $\log {}^\bullet\mathrm{card}\, A_k$ negligible.

V. Non-standard treatment of bridge-solvability

In this section, use techniques from non-standard analysis to prove Theorem 12.

Recall that our formalized version of a non-uniform family of circuits is a non-uniform family of algebraic strategies. The notion of solvability relies on an underlying notion of rough equivalence between a non-uniform process and a uniform one, which we formalize here. First, we define this sort of equivalence as it would apply to exponents:

Definition 29: Suppose $R \in \mathbb{Z}(x_1, \ldots, x_n)$ and $\{S_k\}_{k\in\mathbb{N}}$ is a sequence of elements of $\mathbb{Z}(x_1, \ldots, x_n)$. $R \sim \{S_k\}_k$ if and only if there is a non-negligible function ε such that for all $k \in \mathbb{N}$,

$$\Pr_k \underbrace{\{\bar{\sigma} \in (\mathbb{Z}/(p_k))^n : R(\bar{\sigma}) = S_k(\bar{\sigma})\}}_{A_k} \geq \varepsilon(k) \tag{7}$$

Remark 30: In (7), the symbol $\Pr_k$ refers to the uniform probability measure on $(\mathbb{Z}/(p_k))^n$. Implicit in the defining condition for the sets A_k is that both the RHS and the LHS of the equation within the braces are defined. In particular, the denominators of both $R(\bar{\sigma})$ and $S_k(\bar{\sigma})$ must be non-zero in order for $\bar{\sigma}$ to be an element of A_k.

Remark 31: A necessary and sufficient condition that $R \sim \{S_k\}_k$ is that there exist an $m \in \mathbb{N}$ such that

$$\Pr_k \underbrace{\{\bar{\sigma} \in (\mathbb{Z}/(p_k))^n : R(\bar{\sigma}) = S_k(\bar{\sigma})\}}_{A_k} \geq (\log p_k)^{-m} \quad (8)$$

for infinitely many k. This is a trivial rewrite of (7) using Remark 2.

Proposition 32: Suppose $R_1, R_2, S_k \in \mathbb{Z}(x_1, \ldots, x_n)$ and $R_2 \sim \{S_k \circ R_1\}_k$. If the degree of S_k is a log-sublinear function of p_k (that is the degrees of the numerator and denominator of S_k are log-sublinear in p_k) as $k \to \infty$ then there is an $S \in \mathbb{Z}(x_1, \ldots, x_n)$ such that $S \circ R_1 = R_2$.

In other words, when such an $\{S_k\}$ family exists for a given $(\bar{R}_1, R_2)$ exponent-only derivability problem, R_2 can be derived from $\bar{R}_1$ in a uniform way.

Next we state the more general notion which includes both base and exponent expressions and state the equivalent proposition. The more general version of Proposition 32 proves Theorem 12

Definition 33: Suppose $\bar{u} \in \mathbf{U}^m, \bar{x} \in \mathbf{E}^n$, $F(\bar{u}, \bar{x}) \in \mathrm{B}\langle \bar{u}, \bar{x} \rangle$ and $\{G_k(\bar{u}, \bar{x})\}_{k \in \mathbb{N}}$ a sequence of elements of $\mathrm{B}\langle \bar{u}, \bar{x} \rangle$. Then $F \sim \{G_k\}_k$ if and only if there is a non-negligible function ε such that for all $k \in \mathbb{N}$,

$$\begin{aligned} \Pr_k\{(\bar{\tau},\bar{\sigma}) \in (\mathbb{Z}/(p_k))^m \times (\mathbb{Z}/(p_k))^n : \\ F(\bar{\tau}, \bar{\sigma}) = G_k(\bar{\tau}, \bar{\sigma})\} \geq \varepsilon(k). \end{aligned} \quad (9)$$

Proposition 34: Suppose $R_1, R_2, S_k \in \mathrm{B}\langle \mathbf{U}, \mathbf{E} \rangle$ and $R_2 \sim \{S_k \circ R_1\}_k$. If the degree of S_k is log-sublinear in k then there exists $S \in \mathrm{B}\langle \mathbf{U}, \mathbf{E} \rangle$ such that $R_2 = S \circ R_1$.

A. Generalizing to infinite index

We now strive to prove Propositions 32 and 34.

We apply non-standard analysis techniques, in particular the transfer principle, to extend these definitions and propositions to infinite k. By applying the overspill principle we can then isolate these statements to a single, infinite k. This produces *almost* the environment we expect; the one difference is that we get a definition of solvable based on a non-negligible probability of success of being solved by an allowable derivation, rather than being exactly solved by it. However, we are able to prove that these amount to the same thing. In order to do this, we require some preliminary concepts that restrict the size of algebraic varieties over finite fields.

B. Varieties and Negligible Sets

Let $\mathbf{F}$ be an internal field. We consider *internal* multivariate polynomials $P \in \mathbf{F}[x_1, \ldots, x_n]$ where $n \in {}^\bullet\mathbb{N}$. Elements of $\mathbf{F}[x_1, \ldots, x_n]$ are *internal functions* from the free internal Abelian semigroup generated by $x_1, \ldots, x_n$ into the field $\mathbf{F}$. We also use the notation $\mathbf{F}[\bar{x}]$ to denote the ring $\mathbf{F}[x_1, \ldots, x_n]$. An element $P \in \mathbf{F}[x_1, \ldots, x_n]$ defines a function $\mathbf{F}^n \longrightarrow \mathbf{F}$ which by abuse of language we also denote by P. Note that in general distinct polynomials can define the same function.

Now suppose $\mathbf{F}$ is a *hyperfinite* field and $P \in \mathbf{F}[x_1, \ldots, x_n]$ is a polynomial of degree m. The *variety* defined by P is the set $E \subseteq \mathbf{F}^n$

$$E = \{(x_1, \ldots, x_n) \in \mathbf{F}^n : P(x_1, \ldots, x_n) = 0\} \quad (10)$$

If f is log-sublinear, then for $R \simeq \infty$ and standard hyperinteger k,

$$\frac{{}^\bullet f(R)}{R(\log R)^{-k}} \simeq 0. \quad (11)$$

An internal set $E \subseteq X$ is *negligible* if and only if $\Pr(E)$ is negligible relative to the scale parameter $\log {}^\bullet\mathrm{card}\, X$. The key result we use is the following:

Proposition 35: Suppose $E \subseteq \mathbf{F}^n$ is an algebraic variety defined by a non-trivial polynomial P such that

$$\deg P \leq {}^\bullet f({}^\bullet\mathrm{card}\, \mathbf{F}) \quad (12)$$

where f is log-sublinear. Then E is negligible.
The result is proved in §V-D.

Remark 36: Note that the degree of P need not be standard. Stated contrapositively, Proposition 35 states that if P defines a variety which is non-negligible, then P is trivial.

Remark 37: Stated contrapositively, Proposition 35 states that two polynomials whose degrees are not too large (in the sense of the inequality (12)) and which agree on a non-negligible set are in fact identical.

C. Derivability in the Formal Model

Fix a derivability problem $(\bar{R}_1, R_2)$, and let U, E be the sets of base expressions and exponent expressions, respectively, derivable by the adversary. In other words, U and E consist of base and exponent expressions obtained by composing rational expressions with the R_1 values. We use the notation and context of §IV-B, in particular $\mathcal{S} = \{(G_j, g_j, p_j) : j \in \mathbb{N}\}$ is an admissible system of groups and generators and ${}^\bullet\mathcal{S}$ is the extension obtained by transfer. The following remark is crucial in what follows:

Remark 38: Suppose F is standard and $F \in {}^\bullet U$ (respectively $F \in {}^\bullet E$). Then $F \in U$ (respectively $F \in E$). This is immediate from the transfer principle.

The previous remark is the basic idea behind our use of non-standard analysis. We first consider exponent expressions:

Proof of Proposition 32: Since the set of $\{p_j : j \in \mathbb{N}\}$ is unbounded, there is an $M \simeq \infty$ such that $p_M \simeq \infty$ and

$$R(\bar{\sigma}) - S_M(\bar{\sigma}) = 0 \quad (13)$$

for $\bar{\sigma} \in ({}^\bullet\mathbb{Z}/(p_M))^n$ on a non-negligible set A_M. Let

$$R(\bar{x}) = \frac{R^{\mathrm{num}}(\bar{x})}{R^{\mathrm{den}}(\bar{x})}, \quad S_M(\bar{x}) = \frac{S^{\mathrm{num}}(\bar{x})}{S^{\mathrm{den}}(\bar{x})} \quad (14)$$

so (13) can be regarded as the conjunction

1) $R^{\mathrm{den}}(\bar{\sigma})$ and $S^{\mathrm{den}}(\bar{\sigma})$ are non-zero
2) $R^{\mathrm{num}}(\bar{\sigma})S^{\mathrm{den}}(\bar{\sigma}) = S^{\mathrm{num}}(\bar{\sigma})R^{\mathrm{den}}(\bar{\sigma})$

The result now follows from Proposition 35 and the transfer principle. ∎

Proof of Proposition 34: There is an $M \simeq \infty$ such that $p_M \simeq \infty$ and the set

$$\{(\bar{\tau}, \bar{\sigma}) \in ({}^\bullet\mathbb{Z}/(p_M))^m \times ({}^\bullet\mathbb{Z}/(p_M))^n : F(\bar{\tau}, \bar{\sigma}) = G_M(\bar{\tau}, \bar{\sigma})\}$$

has non-negligible probability. Equivalently $(\bar{\tau}, \bar{\sigma}) \in ({}^\bullet\mathbb{Z}/(p_M))^m \times ({}^\bullet\mathbb{Z}/(p_M))^n$ such that

$$\tau_1^{R_1(\bar{\sigma})} \cdots \tau_m^{R_m(\bar{\sigma})} = \tau_1^{S_1(\bar{\sigma})} \cdots \tau_m^{S_m(\bar{\sigma})} \tag{15}$$

has non-negligible probability, where

$$G_M(\bar{u}, \bar{x}) = u_1^{S_1(\bar{x})} \cdots u_m^{S_m(\bar{x})}$$

Choose a generator ρ for G_M. Then (15) can be expressed as

$$\rho^{\alpha_1 R_1(\bar{\sigma}) + \cdots + \alpha_m R_m(\bar{\sigma})} = \rho^{\alpha_1 S_1(\bar{\sigma}) + \cdots + \alpha_m S_m(\bar{\sigma})} \tag{16}$$

which holds for $(\bar{\alpha}, \bar{\sigma})$ ranging over a subset A_M of $({}^\bullet\mathbb{Z}/(p_M))^m \times ({}^\bullet\mathbb{Z}/(p_M))^n$ of non-negligible probability. Therefore

$$\alpha_1(R_1(\bar{\sigma}) - S_1(\bar{\sigma})) + \cdots + \alpha_m(R_m(\bar{\sigma}) - S_m(\bar{\sigma})) = 0.$$

for $(\bar{\alpha}, \bar{\sigma}) \in A_M$. Thus for all k, $1 \le k \le m$, $R_k(\bar{x}) - S_k(\bar{x}) = 0$ which proves the result. ∎

D. Negligibility of Algebraic Varieties

We now turn to the main technical result which limits the size of algebraic varieties defined by polynomials of log-sublinear degree in the field size.

Proposition 39: Suppose $E \subseteq \mathbf{F}^n$ is an algebraic variety defined by a non-trivial polynomial P. Then

$${}^\bullet\mathrm{card}\, E \le n \deg P ({}^\bullet\mathrm{card}\, \mathbf{F})^{n-1} \tag{17}$$

Proof: Let $m = \deg P$. The proof is by induction on n. P is of the form

$$P(\bar{x}, y) = {}^\bullet\sum\nolimits_{k \le m} a_k P_k(\bar{x}) y^k, \tag{18}$$

where $P_k(\bar{x}) \in \mathbf{F}[x_1, \ldots, x_{n-1}]$ is a polynomial of degree at most m. Now for each $\bar{a} \in \mathbf{F}^{n-1}$, one of the following holds:

1) The polynomial in one variable $P(\bar{a}, y)$ is identically 0 or equivalently,

   $$P_0(\bar{a}) = P_1(\bar{a}) = \cdots = P_m(\bar{a}) = 0.$$

   By the inductive hypothesis there are at most $(n-1) \times m \times ({}^\bullet\mathrm{card}\, \mathbf{F})^{n-2}$ elements $\bar{a} \in \mathbf{F}^{n-1}$ in this case and each one contributes ${}^\bullet\mathrm{card}\, \mathbf{F}$ solutions to $P(\bar{a}, b) = 0$
2) There are possibly as many as $({}^\bullet\mathrm{card}\, \mathbf{F})^{n-1}$ elements $\bar{a}$ in this case, but each one contributes at most m solutions to $P(\bar{a}, b) = 0$ as b ranges over $\mathbf{F}$.

Altogether therefore, there are at most

$$(n-1)m({}^\bullet\mathrm{card}\, \mathbf{F})^{n-1} + ({}^\bullet\mathrm{card}\, \mathbf{F})^{n-1} m = nm({}^\bullet\mathrm{card}\, \mathbf{F})^{n-1}$$

elements in E. In case (1), therefore $P(\bar{a}, b) = 0$ has at most $({}^\bullet\mathrm{card}\, \mathbf{F})^{n-1} \times m$ solutions as $\bar{a}, b$ range over $\mathbf{F}^{n-1}$, $\mathbf{F}$ respectively. ∎

Henceforth we assume without further mention that $\mathbf{F}$ is a hyperfinite field such that ${}^\bullet\mathrm{card}\, \mathbf{F} \simeq \infty$. In this section, $\mathbf{F}$ will be instantiated with a field ${}^\bullet\mathbb{Z}/(p)$ with p a infinite prime.

Proof of Proposition 35: Let $m = \deg P$. By Proposition 39 and the assumption that ${}^\bullet\mathrm{card}\, \mathbf{F} \simeq \infty$,

$$\begin{aligned}
\Pr(E)(\log {}^\bullet\mathrm{card}\, \mathbf{F})^k &= \frac{{}^\bullet\mathrm{card}\, E}{{}^\bullet\mathrm{card}\, \mathbf{F}^n} (\log {}^\bullet\mathrm{card}\, \mathbf{F})^k \\
&\le \frac{nm\, {}^\bullet\mathrm{card}\, \mathbf{F}^{n-1}}{{}^\bullet\mathrm{card}\, \mathbf{F}^n} (\log {}^\bullet\mathrm{card}\, \mathbf{F})^k \\
&\le n\, \frac{f({}^\bullet\mathrm{card}\, \mathbf{F})}{{}^\bullet\mathrm{card}\, \mathbf{F}} (\log {}^\bullet\mathrm{card}\, \mathbf{F})^k \simeq 0.
\end{aligned}$$

∎

Another consequence of Proposition 35 is that it gives rise to a notion of "defined almost everywhere" that applies to log-sublinear degree rational function families. A partial internal function f on X is *defined almost everywhere* if and only if $X \setminus \mathrm{dom}\, f$ is a negligible set (relative to $\log {}^\bullet\mathrm{card}\, X$).

Remark 40: Suppose $\mathbf{F}$ is a hyperfinite field such that ${}^\bullet\mathrm{card}\, \mathbf{F} \in {}^\bullet\mathbb{N} \setminus \mathbb{N}$ and $R(\bar{x}) = P(\bar{x})/Q(\bar{x})$ where $0 \ne Q(\bar{x}) \in \mathbf{F}[x]$ and $\deg Q(\bar{x}) \le Cf({}^\bullet\mathrm{card}\, \mathbf{F})$ with nf log-sublinear. Then R is almost everywhere defined.

Proof: P is defined precisely when $Q(\bar{x}) \ne 0$ which by Proposition 35 holds everywhere except a negligible set. ∎

VI. Restricting to the Diffie-Hellman algebra

The formal polynomial model thus far developed unfortunately falls short of what we need for protocol analysis. As Dougherty and Guttman point out, the notion that all exponents other than 0 have inverses cannot be simply expressed in an equational theory [11]. Worse, any reasonable attempt at emulating this formal model with an algebra would be problematic because the exponents would form a ring structure, and unification, a key technique in automated exploratory protocol analysis, is not known to be decidable for rings.

In this section we present the proof of Theorem 15, that monomial solvability is equivalent to formal solvability for monomial derivation problems.

The results of Proposition 42 and Corollary 43 are the main results supporting this conclusion. They state that monomials that can be expressed as polynomials (respectively, rational expressions) of monomials can be expressed as monomials of those monomials.

A. Monomials and Polynomials

Suppose $r, n \in \mathbb{Z}$ and $A \in \mathbf{M}_{r \times n}(\mathbb{Z})$. Let

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{r1} & \alpha_{r2} & \cdots & \alpha_{rn}. \end{bmatrix} = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_r \end{bmatrix} \tag{19}$$

$\overline{M}_A(\bar{x})$ is the vector of monomials (displayed as a column vector for readability):

$$\overline{M}_A(\bar{x}) = \begin{bmatrix} M_{A_1}(\bar{x}) \\ M_{A_2}(\bar{x}) \\ \vdots \\ M_{A_r}(\bar{x}) \end{bmatrix} = \begin{bmatrix} x_1^{\alpha_{11}} x_2^{\alpha_{12}} \cdots x_n^{\alpha_{1n}} \\ x_1^{\alpha_{21}} x_2^{\alpha_{22}} \cdots x_n^{\alpha_{2n}} \\ \vdots \\ x_1^{\alpha_{r1}} x_2^{\alpha_{r2}} \cdots x_n^{\alpha_{rn}} \end{bmatrix} \tag{20}$$

As a special case, if $\bar{\alpha} \in \mathbf{M}_{1\times n}(\mathbb{Z})$ (i.e. $\bar{\alpha}$ is a row vector with n entries), then

$$M_{\bar{\alpha}}(\bar{x}) = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

We regard $\overline{M}_A(\bar{x})$ as a mapping $\mathbf{F}^n \longrightarrow \mathbf{F}^r$. Since each component M_ℓ of $\overline{M}_A$ is almost everywhere defined and the number of components is standard, $\overline{M}_A$ is almost everywhere defined. The proof of the following is a straightforward computation:

Proposition 41: If $C \in \mathbf{M}_{r\times n}(\mathbb{Z})$ and $D \in \mathbf{M}_{r\times n}(\mathbb{Z})$ then

$$\overline{M}_C(\bar{x}) \cdot \overline{M}_D(\bar{x}) = \overline{M}_{C+D}(\bar{x}) \tag{21}$$

where the product is the coordinatewise product. If $B \in \mathbf{M}_{s\times r}(\mathbb{Z})$ and $A \in \mathbf{M}_{r\times n}(\mathbb{Z})$, then

$$\overline{M}_B\left(\overline{M}_A(\bar{x})\right) = \overline{M}_{B\cdot A}(\bar{x}). \tag{22}$$

In particular, if $\bar{\beta} \in \mathbf{M}_{1\times r}(\mathbb{Z})$

$$\overline{M}_{\bar{\beta}\cdot A}(\bar{x}) = M_{\bar{\beta}}\overline{M}_A(\bar{x}) = M_{A_1}^{\beta_1}(\bar{x}) M_{A_2}^{\beta_2}(\bar{x}) \cdots M_{A_r}^{\beta_r}(\bar{x}) \tag{23}$$

We now consider composition with polynomials. Suppose $P(\bar{y}) \in \mathbf{F}[y_1, \ldots, y_r]$ is a polynomial of degree m. Thus

$$P(y_1, \ldots, y_r) = \sum_{|\bar{\beta}|\le m} c_{\bar{\beta}} y_1^{\beta_1} y_2^{\beta_2} \cdots y_r^{\beta_r} = \sum_{|\bar{\beta}|\le m} c_{\bar{\beta}} M_{\bar{\beta}}(\bar{y}) \tag{24}$$

If A is an $r \times n$ matrix as in (19), then by (23),

$$\begin{aligned} P\left(\overline{M}_A(\bar{x})\right) &= \sum_{|\bar{\beta}|\le m} c_{\bar{\beta}} M_{\bar{\beta}}(M_A(\bar{x})) \\ &= \sum_{\bar{\beta}} c_{\bar{\beta}} M_{\bar{\beta}\cdot A}(\bar{x}) \\ &= \sum_{\bar{\gamma}} \left\{ \sum_{\bar{\beta}\cdot A = \bar{\gamma}} c_{\bar{\beta}} \right\} M_{\bar{\gamma}}(\bar{x}). \end{aligned}$$

Since the family $M_{\bar{\gamma}}(\bar{x})$ of monomials in the vector space $\mathbf{F}[x_1, \ldots, x_n]$ is linearly independent, we have shown:

Proposition 42: If $P(\bar{y}) = \sum_{\bar{\beta}} c_{\bar{\beta}} \bar{y}^{\bar{\beta}} \in \mathbf{F}[y_1, \ldots, y_r]$ and $A \in \mathbf{M}_{r\times n}(\mathbb{Z})$ is such that

$$P\left(M_{A_1}(\bar{x}), M_{A_2}(\bar{x}), \ldots, M_{A_r}(\bar{x})\right) = 0$$

then for every $\bar{\gamma}$,

$$\sum_{\bar{\beta}\cdot A = \bar{\gamma}} c_{\bar{\beta}} = 0. \tag{25}$$

An immediate corollary is the conclusion that polynomial identities between monomials are essentially monomial identities. This result has the following significance: an adversary that can compute arbitrary polynomials on monomials has can produce exactly those monomials that can be produced by an adversary restricted to computing monomials.

Corollary 43: Suppose

$$R(\bar{y}) = \frac{\sum_{\bar{\beta}} c_{\bar{\beta}} M_{\bar{\beta}}(\bar{y})}{\sum_{\bar{\beta}} d_{\bar{\beta}} M_{\bar{\beta}}(\bar{y})} \in \mathbf{F}(y_1, \ldots, y_r), \tag{26}$$

$A \in \mathbf{M}_{r\times n}(\mathbb{Z})$ and $\bar{\gamma} \in \mathbf{M}_{1\times n}(\mathbb{Z})$ are such that

$$R\left(M_{A_1}(\bar{x}), M_{A_2}(\bar{x}), \ldots, M_{A_r}(\bar{x})\right) = M_{\bar{\gamma}}(\bar{x}) \tag{27}$$

Then there is a $\bar{\tau} \in \mathbf{M}_{1\times r}(\mathbb{Z})$ such that $\bar{\gamma} = \bar{\tau} \cdot A$ and for any such $\bar{\tau}$

$$M_{A_1}^{\tau_1}(\bar{x}) M_{A_2}^{\tau_2}(\bar{x}) \cdots M_{A_r}^{\tau_r}(\bar{x}) = M_{\bar{\tau}}(\overline{M}_A(\bar{x})) = M_{\bar{\gamma}}(\bar{x}). \tag{28}$$

Proof: From (26) and (27) it follows that

$$\begin{aligned} \sum_{\bar{\beta}} d_{\bar{\beta}} M_{\bar{\gamma}+\bar{\beta}\cdot A}(\bar{x}) &= M_{\bar{\gamma}}(\bar{x}) \sum_{\bar{\beta}} d_{\bar{\beta}} M_{\bar{\beta}}(\overline{M}_A(\bar{x})) \\ &= \sum_{\bar{\beta}} c_{\bar{\beta}} M_{\bar{\beta}}(\overline{M}_A(\bar{x})) \\ &= \sum_{\bar{\beta}} c_{\bar{\beta}} M_{\bar{\beta}\cdot A}(\bar{x}) \end{aligned}$$

By Proposition 42, for every $\bar{\tau}$,

$$\sum_{\bar{\gamma}+\bar{\beta}\cdot A = \bar{\tau}} d_{\bar{\beta}} M_{\bar{\gamma}+\bar{\beta}\cdot A}(\bar{x}) = \sum_{\bar{\beta}\cdot A = \bar{\tau}} c_{\bar{\beta}} M_{\bar{\beta}\cdot A}(\bar{x}) \tag{29}$$

Let $\bar{\tau}$ be such that $\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}} \neq 0$. Such a $\bar{\tau}$ exists, for otherwise the rational function R would be identically 0 which is impossible by (27). Choose some $\bar{\rho}$ such that $\bar{\gamma} + \bar{\rho} \cdot A = \bar{\tau}$; such an index exists for otherwise the sum $\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}}$ would be 0. If $\bar{\gamma} + \bar{\beta} \cdot A = \bar{\tau}$, then

$$M_{\bar{\gamma}+\bar{\rho}\cdot A}(\bar{x}) = M_{\bar{\gamma}+\bar{\beta}\cdot A}(\bar{x}).$$

Similarly choose some $\bar{\kappa}$ such that $\bar{\kappa} \cdot A = \tau$. If $\bar{\beta} \cdot A = \bar{\tau}$

$$M_{\bar{\kappa}\cdot A}(\bar{x}) = M_{\bar{\tau}}(\bar{x}) = M_{\bar{\beta}\cdot A}(\bar{x})$$

Then from (29).

$$\left(\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}}\right) M_{\bar{\gamma}+\bar{\rho}\cdot A}(\bar{x}) = \left(\sum_{\bar{\beta}\cdot A=\bar{\tau}} c_{\bar{\beta}}\right) M_{\bar{\kappa}\cdot A}(\bar{x}) \tag{30}$$

Thus

$$\begin{aligned} M_{\bar{\gamma}}(\bar{x}) &= \frac{\sum_{\bar{\beta}\cdot A=\bar{\tau}} c_{\bar{\beta}}}{\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}}} \frac{M_{\bar{\kappa}\cdot A}(\bar{x})}{M_{\bar{\rho}\cdot A}(\bar{x})} \\ &= \frac{\sum_{\bar{\beta}\cdot A=\bar{\tau}} c_{\bar{\beta}}}{\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}}} M_{A_1}^{\kappa_1-\rho_1}(\bar{x}) \cdots M_{A_r}^{\kappa_r-\rho_r}(\bar{x}) \end{aligned}$$

which is of the form (28). ∎

VII. Conclusion

In this paper we justify a simple algebra for the modeling of Diffie-Hellman protocols. The algebra represents multiplication of exponents and exponentiation but does not represent addition of exponents or multiplication of bases. We justify our model by linking it to a standard computational model, and show a link between the concept of derivability in the computational model and in our model. To recap:

1) The **computational model** is consistent with state-of-the art methods of expressing the difficulty of computational Diffie-Hellman and related problems.
2) The **asymptotic polynomial model** is a direct analogue of the computational model where circuits are replaced by strategies based on randomized, explicit rational functions. Although this notion is not shown equivalent to the computational notion, crossing the divide of this sort is implicit, and we do so as directly and clearly as possible.
3) The **formal polynomial model** deals with randomly selected values as abstract variables and concerns formal derivation using a uniform rational expression-based strategy. We prove that solvability in this model is equivalent to solvability in the asymptotic polynomial model.
4) The **monomial model** is equivalent to an algebra-based model of Diffie-Hellman derivability. We prove that monomial solvability is equivalent to formal solvability for monomial derivation problems. In other words, by restricting the model we *necessarily* lose the expressive power to describe non-monomial derivation problems, but apart from this, the notion of solvability is unchanged.

References

[1] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *J. Cryptology*, 20(3):395, 2007.

[2] S. Albeverio, J.E. Fenstad, R. Höegh-Kron, and T. Lindström. *Nonstandard Analysis in Stochastic Analysis and Mathematical Physics*. Academic Press, New York, 1986.

[3] Michael Backes, Birgit Pfitzmann, and Michael Waidner. A composable cryptographic library with nested operations. In Sushil Jajodia, Vijayalakshmi Atluri, and Trent Jaeger, editors, *ACM Conference on Computer and Communications Security*, pages 220–230. ACM, 2003.

[4] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM Conference on Computer and Communications Security*, pages 62–73. ACM, 1993.

[5] Bruno Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In *CSFW*, pages 82–96. IEEE Computer Society, 2001.

[6] Michele Boreale and Maria Grazia Buscemi. Symbolic analysis of crypto-protocols based on modular exponentiation. In Branislav Rovan and Peter Vojtás, editors, *MFCS*, volume 2747 of *Lecture Notes in Computer Science*, pages 269–278. Springer, 2003.

[7] Emmanuel Bresson, Yassine Lakhnech, Laurent Mazaré, and Bogdan Warinschi. *Formal Models and Techniques for Analyzing Security Protocols*, chapter Computational Soundness - The Case of Diffie-Hellman Keys. IOS Press, 2011.

[8] Ran Canetti. *Encyclopedia of Cryptography and Security*, chapter Decisional Diffie-Hellman Assumption. Springer-Verlag, 2005.

[9] Ran Canetti and Jonathan Herzog. Universally composable symbolic security analysis. *J. Cryptology*, 24(1):83–147, 2011.

[10] W. Diffie and M. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644 – 654, nov 1976.

[11] Daniel J. Dougherty and Joshua D. Guttman. Symbolic protocol analysis for Diffie-Hellman. *CoRR*, abs/1202.2168, 2012.

[12] Santiago Escobar, Catherine Meadows, and José Meseguer. Maude-npa: Cryptographic protocol analysis modulo equational properties. In Alessandro Aldini, Gilles Barthe, and Roberto Gorrieri, editors, *FOSAD*, volume 5705 of *Lecture Notes in Computer Science*, pages 1–50. Springer, 2007.

[13] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *J. Comput. Syst. Sci.*, 28(2):270–299, 1984.

[14] Jean Goubault-Larrecq, Muriel Roger, and Kumar Neeraj Verma. Abstraction and resolution modulo ac: How to verify diffie-hellman-like protocols automatically. *J. Log. Algebr. Program.*, 64(2):219–251, 2005.

[15] Deepak Kapur, Paliath Narendran, and Lida Wang. An e-unification algorithm for analyzing protocols that use modular exponentiation. In Robert Nieuwenhuis, editor, *RTA*, volume 2706 of *Lecture Notes in Computer Science*, pages 165–179. Springer, 2003.

[16] Ralf Küsters and Tomasz Truderung. Using proverif to analyze protocols with diffie-hellman exponentiation. In *CSF*, pages 157–171. IEEE Computer Society, 2009.

[17] Daniele Micciancio and Bogdan Warinschi. Completeness theorems for the abadi-rogaway logic of encrypted expressions. *Journal of Computer Security*, 12(1):99–129, 2004. Preliminary version in WITS 2002.

[18] Edward Nelson. Internal set theory: A new approach to nonstandard analysis. *Bull. Amer. Math. Soc*, pages 1165–1198, 1977.

[19] John D. Ramsdell and Joshua D. Guttman. CPSA, a cryptographic protocol shapes analyzer. 2009.

[20] Benedikt Schmidt, Simon Meier, Cas J. F. Cremers, and David A. Basin. Automated analysis of diffie-hellman protocols and advanced security properties. In Stephen Chong, editor, *CSF*, pages 78–94. IEEE, 2012.

[21] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *EUROCRYPT*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer, 1997.

[22] Terence Tao. Ultraproducts as a bridge between discrete and continuous analysis, 2013.

Appendix

A. Non-standard view of computational derivability

In this section, we give a non-standard analysis-based view of the computational model of DH derivability. This allows us to state computational derivability without direct reliance on asymptotic behavior and parameters. This may be of independent interest, as explicit handling of security parameters is frequently necessary in cryptographic papers so as to remain faithful to asymptotic notions of computation, but is rarely directly illuminating.

We have already discussed a non-standard treatment of admissible systems, probability, and negligible functions. We thus need only explore the idea of infinite indices in polynomially bounded non-uniform circuit families. This is done by applying the transfer operator to everything in sight. In keeping with our notation, we use ${}^\bullet\mathcal{C}$ to denote the class of circuits in the universe ${}^\circ\mathcal{U}$, ${}^\bullet|\cdot|$ denotes the size function.

If $\mathcal{A} = \{A_k\} \in \mathcal{PNC}$ is a standard polynomially bounded non-uniform circuit family, by transfer we simply think of A_k as being of size $\leq \rho(k)$ even when $k \simeq \infty$. Using non-standard analysis, we can restate the condition with a single infinite index.

In the following $\mathfrak{P}$ denotes the set of primes.

Proposition 44: A derivation problem $(\bar{R}_1, R_2)$ is *solvable* if and only if for some $k \simeq \infty$, there is a $p \in {}^\bullet\mathfrak{P}$ such that $0 \ll p/2^k \ll \infty$ and an $A \in {}^\bullet\mathcal{C}$ such that for some standard

m, $|A| \leq k^m$ and

$$\Pr[\bar{x} \leftarrow (\mathbb{Z}/(p)); v \leftarrow A(\bar{R}_1(\bar{x})) : v = R_2(\bar{x})\}] \tag{31}$$

is not k-negligible.

Proof: If the derivation problem is solvable in the sense of Definition 5, then overspill implies the stated condition. Conversely, if the stated condition holds, there are $k \simeq \infty$, standard constants $0 < c \leq C < \infty$ such that $c \leq p/2^k \leq C$, a standard positive integer m and a circuit A such that $\rho(A) \leq k^m$

$$\Pr[\bar{x} \leftarrow (\mathbb{Z}/(p)); v \leftarrow A(\bar{\alpha}(\bar{x})) : v = \beta(\bar{x})\}] \geq k^{-m} \tag{32}$$

Therefore the following formula with standard parameters $\bar{\alpha}, \beta, c, C$ is valid in $^\circ\mathfrak{V}$:

$$\begin{aligned} &\forall^{\mathrm{st}}\ell,\ \exists k \geq \ell,\ \exists p \in {}^\bullet\mathfrak{P},\ \exists A \in {}^\bullet\mathcal{PNC}, \\ &\quad c \leq p/2^k \leq C \\ &\quad \text{and} \\ &\quad \Pr[\bar{x} \leftarrow (\mathbb{Z}/(p)); v \leftarrow A(\bar{\alpha}(\bar{x})) : v = \beta(\bar{x})\}] \geq k^{-m} \end{aligned} \tag{33}$$

By transfer, we obtain the following completely standard formula.

$$\begin{aligned} &\forall \ell \in \mathbb{N},\ \exists k \geq \ell,\ \exists p \in \mathfrak{P},\ \exists A \in \mathcal{PNC}, \\ &\quad c \leq p/2^k \leq C \\ &\quad \text{and} \\ &\quad \Pr[\bar{x} \leftarrow (\mathbb{Z}/(p)); v \leftarrow A(\bar{\alpha}(\bar{x})) : v = \beta(\bar{x})\}] \geq k^{-m} \end{aligned} \tag{34}$$

This is precisely the condition for solvability. ■

Note that since Proposition 44 refers only to a single infinite k, and since the properties observed in subsection IV-B apply to any infinite k, this allows us to view the environment in the simple way we described at the beginning of this section: as a single environment, with no overly specific properties.