Journal of Automata, Languages and Combinatorics **u** (v) w, x–y
© Otto-von-Guericke-Universität Magdeburg

Random polynomial-time attacks and Dolev-Yao models

Mathieu Baudet[1]
LSV — CNRS UMR 8643 & INRIA Futurs projet SECSI & ENS Cachan
61, av. du président Wilson 94235 Cachan Cedex, France
e-mail: baudet@lsv.ens-cachan.fr

ABSTRACT

In this paper we present an extension of Dolev-Yao models for security protocols with a notion of random polynomial-time (Las Vegas) computability. First we notice that Dolev-Yao models can be seen as transition systems, possibly infinite. We then extend these transition systems with computation times and probabilities. The extended models can account for normal Dolev-Yao transitions as well as nonstandard operations such as inverting a one-way function. Our main contribution consists of showing that under reasonable assumptions the extended models are equivalent to standard Dolev-Yao models as far as (safety) security properties are concerned.

Keywords: Cryptographic protocols, random polynomial time, Dolev-Yao model, Markov decision processes

1. Introduction

Proving the security of cryptographic protocols has been a major concern ever since flaws were first discovered in some established protocols, the most well-known example being Lowe's attack on the Needham-Schroeder Protocol [23]. Rigorous approaches now exist and have allowed for the analysis of many protocols with respect to various security models. As a matter of fact, two families of models with little in common have been used for years by two different communities.

Computational (or *cryptographic*) models define security in a semantic way by requiring the probability of success of any attacker to be negligible [17, 38]. The class of attacks considered here includes virtually all logical attacks, as soon as they can be implemented by a probabilistic polynomial-time Turing machine.

Formal (or *logical*) models are used by the community of *formal methods* and typically include the Dolev-Yao model [16] and cryptographic process calculi such as the spi-calculus [1]. Formal models are able to capture a variety of attacks on protocols, resulting from complex interactions between an active attacker and a possibly unbounded number of parallel sessions. They are now the basis for many automatic

[1]Partially supported by the the RNTL projects EVA and Prouvé, the ACI Sécurité Informatique Rossignol, the ACI Cryptologie Psi-Robuste, and the ACI jeunes chercheurs "Sécurité informatique, protocoles cryptographiques et détection d'intrusions".

tools used to verify protocols ([25, 30, 18, 28, 31, 10, 7, 9] and many others). Yet, as opposed to computational models, formal models only consider adversaries that are limited to a given set of tractable actions.

Motivated by these observations, significant efforts have been made to relate the two views of cryptography [3, 2, 22, 12, 21, 6, 24, 26, 5, 20, 27, 13, 35]. Most of this work[2] proves the computational soundness of various formal models provided that standard assumptions hold on the cryptographic schemes. The motivation for this is clear: once a formal model has been proved computationally sound, automatic analyzers based on this model yield computationally valid proofs of security.

Recently, a different approach was initiated by Zunino and Degano [39]. Here a cryptographic process calculus is introduced and the capability of the formal attacker is augmented with nonstandard operations, such as decrypting a message without the appropriate key. The intuition that nonstandard operations should be computationally intractable is captured by giving the calculus a probabilistic semantics and assigning those operations any negligible probabilities of success. Zunino and Degano then prove that secrecy in the model with enhanced attacker capabilities is equivalent that secrecy in the initial Dolev-Yao-like model.

The approach of Zunino and Degano differs from [3, 2, 22, 12, 21, 6, 24, 26, 5, 20, 27, 13, 35] as they do not aim at directly proving the computational soundness of their initial Dolev-Yao model. Yet it is an interesting question to ask what happens to the security of Dolev-Yao systems when those are augmented with computational flavors *e.g.* probabilities. Results such as Zunino and Degano's tend to confirm that current formal models need not be extended before proving their computational soundness—at least not in an asymptotic computational setting.

In this paper we aim to generalize the result of Zunino and Degano [39] in several manners. First, we extend Dolev-Yao models with a notion of probabilistic computational time, rather than just probabilities of success. It is still possible to recover the probabilistic model of [39] by restricting the times of computations to be either 0 or ∞.

Second and more importantly, we do not consider a particular formal model but emphasize that the result (*i.e.* the equivalence between the extended and initial models) holds for all Dolev-Yao models, as soon as these can be embedded in transition systems and security is stated as a safety property. This abstract point of view allows us to clarify a number of hypotheses. In particular we introduce the so-called *uniform intractability* assumption, which requires intuitively that all nonstandard transitions are eventually intractable *at the same time i.e.* for the same values of the complexity parameter.

Outline of the paper. In Section 2, we describe an abstract view of a general class of formal models including Dolev-Yao variants. The abstraction consists in modeling Dolev-Yao security as the unreachability of certain unsafe states—where for instance a secret has been illegitimately obtained—in possibly infinite transition systems.

[2] Lincoln *et al.* [22] and subsequent work [24, 35] detail a logical framework for (direct) computational proofs of protocols.

In Section 3, we only consider the extension of the simplistic models of Section 2 to include deterministic computation times for each action. This is done by labeling transitions by functions of a complexity parameter n. Usual operations of the Dolev-Yao intruder are modeled by polynomially-bounded (polynomial) times. The benefit of this extension is to account for nonstandard operations—such as guessing a key or breaking a cryptographic primitive—by means of new transitions labeled with non-polynomial times. Security is defined as the fact that no unsafe state can be reached in polynomial time. Our contribution here lies in proving that security in the extended model is equivalent to security in the underlying Dolev-Yao model.

We deal with the expected generalization to a probabilistic framework in Section 4. There tractable operations are those for which a random polynomial-time (Las Vegas) algorithm exists. Reachability is defined as the results of $1\frac{1}{2}$-player games between the attacker and a probabilistic opponent (*a.k.a.* Markov decision processes). We show again that security in the underlying Dolev-Yao models is equivalent to security in the extended models, defined as the fact that no strategy can reach the set of unsafe states with a non-negligible probability.

2. Dolev-Yao models and transition systems

Dolev-Yao models distinguish themselves from other models by several particularities.

- First cryptographic primitives are assumed to be perfect: there is no way to retrieve any information about a message from its hash-code or from its encryption unless we have the adequate key.
- More generally Dolev-Yao models suppose that the attacker is not interested in—and does not exploit—partial or probabilistic information. In other words, messages are considered secret unless they are entirely and definitely compromised.
- The network is modeled in the most pessimistic way. Namely the principals' messages can not only be read but also deleted whereas new messages can be forged by the attacker. In this context, it is natural to assimilate the network to the intruder itself.

These choices often lead to modeling the principals and the attacker by a finite set of *rules* or *actions*. Each rule intuitively states that under certain conditions about previously seen messages, the network might learn some other messages, either by receiving them from a principal or by inferring them from its knowledge.

In the remaining of this section we illustrate the link between Dolev-Yao models and transition systems through the example of the Diffie-Hellman Key-Exchange protocol [15].

Assume that a prime number p, a generator g of the cyclic group $\mathbb{Z}_p^*$ and some acknowledgment message Ack have been chosen in advance. We write $\{X\}_K$ for the encryption of message X with key K by some symmetric encryption algorithm. One session of the protocol consists of two principals A and B exchanging the three following messages:

1. $A \to B : \ g^{N_a}$
2. $B \to A : \ g^{N_b}$
3. $A \to B : \ \{Ack\}_{g^{N_a N_b}}$

From the principals' point of view, the different steps of the protocol considered here work as follows:

(i) first, A draws a random number N_a, computes the modular exponentiation g^{N_a} and sends it to B;

(ii) upon receiving g^{N_a}, B draws another random number N_b and sends g^{N_b} to A;

(iii) then, A computes $(g^{N_b})^{N_a} = g^{N_a N_b}$ and uses this number as a key to compute $\{Ack\}_{g^{N_a N_b}}$ which is sent to B;

(iv) finally, B computes $g^{N_a N_b} = (g^{N_a})^{N_b}$, uses this number to decrypt the final message and checks the obtained plaintext against Ack.

The claim of the protocol is that at the end of a successful session $g^{N_a N_b}$ is a secret shared between the two principals A and B. For one session this is known as the intractability of the (computational/decisional) Diffie-Hellman problem.

In order to study several sessions in parallel, one can resort to an abstracted Dolev-Yao model. A possible instantiation of this model is sketched as follows. Messages are terms defined by

$$\begin{array}{lll} M ::= N & & \text{nonces } N \in \mathcal{N} \\ \quad | \ Ack & & \text{acknowledgment message} \\ \quad | \ \{M_1\}_{M_2} & & \text{symmetric encryption} \\ \quad | \ e(M) & & \text{modular exponentiation of } g \text{ by } M \\ \quad | \ M_1 \oplus M_2 & & \text{product inside exponents} \end{array}$$

where the symbol $\oplus$ satisfies the equations for associativity and commutativity (AC)

$$(M_1 \oplus M_2) \oplus M_3 = M_1 \oplus (M_2 \oplus M_3) \qquad M_1 \oplus M_2 = M_2 \oplus M_1,$$

but the other function symbols are free. In other words, equality between terms is axiomatized by the above two equations and the usual axioms for equality. In particular, the equality $\{M_1\}_{\{M_2\}} = \{M_1'\}_{\{M_2'\}}$ holds iff $M_1 = M_1'$ and $M_2 = M_2'$. Formal models featuring algebraic theories such as AC or XOR have been studied among others in [29, 14, 37]; practical results on the Group Diffie-Hellman protocol were achieved notably in [33, 14, 36].

Each principal $i \in \mathcal{I}$ has an *internal state* q_i which is a set of *sessions* s in which it is involved. Each session $s = (s_{role}, s_{name}, s_{step}, s_{nonce}, s_{data}) \in q_i$ consists of

- the principal's role in the protocol $s_{role} \in \{A, B\}$,
- the name of his correspondent s_{name},
- the number of the expected next message in the protocol $s_{step} \in \{1, 2, 3, done\}$,
- the private nonce s_{nonce},
- the received data s_{data} (for storing the $e(N)$ sent by the correspondent).

The intruder's state is the set of all messages E that he knows (from the network or from its deductions). The global state of the system is the product of the states of all the principals and the intruder $q = ((q_i)_{i\in\mathcal{I}}, E)$. The transitions between global states are described using a finite number of *communication* rules and *deduction* rules. Each rule yields a (possibly infinite) number of transitions $q \to q'$ between global states. Specifically, communication rules describe the behavior of principals in the protocol. In our example above, step (iii) of the protocol (involving messages 2 and 3, seen by the role A) works as follows:

> if a principal i has initiated a session as A with some principal j, its private session number is N_a and the network knows a message $e(N)$, then i may accept $e(N)$ as an incoming message and reply by sending the message $\{Ack\}_{e(N_a\oplus N)}$.

Formally this is written: for every $i, j, (q_\ell)_{\ell\in\mathcal{I}}, E, s, N_a, N$,

> if $s = (A, j, 2, N_a, s_{data}) \in q_i$ and $e(N) \in E$
> then we have the transition $((q_\ell), E) \longrightarrow ((q'_\ell), E')$
> where $q'_\ell = q_\ell$ for all $\ell \neq i$, $q'_i = q_i - \{s\} \cup \{s'\}$, $s' = (A, j, done, N_a, e(N))$
> and $E' = E \cup \{\ \{Ack\}_{e(N_a\oplus N)}\}$.

The deduction rules are protocol independent. They describe the possible deductions for the attacker. Typical deduction rules are: (for every $(q_i)_{i\in\mathcal{I}}, E, M, M', K$)

- encryption: if $M \in E$ and $K \in E$ then $((q_i), E) \longrightarrow ((q_i), E \cup \{\{M\}_K\})$,
- decryption: if $\{M\}_K \in E$ and $K \in E$ then $((q_i), E) \longrightarrow ((q_i), E \cup \{M\})$,
- exponentiation: if $e(M) \in E$ and $M' \in E$ then we have the transition $((q_i), E) \longrightarrow ((q_i), E \cup \{e(M \oplus M')\})$.

Our point is that these rules describe an (infinite countable) transition system. In general, there exist many ways to model the security of protocols in terms of transition systems (see *e.g.* [9] or [8] for systematic approaches using process calculi). In many cases, security can be defined as a *safety property*, *i.e.* the fact that certain *unsafe* states are unreachable. Unsafe states of the previous examples are the states $q = ((q_i), E)$ such that E contains a presumably secret term $g^{N_a N_b}$. We will concentrate on this notion of security in the following. This includes for instance secrecy and various forms of authentication [4].

In the sequel we do not assume that the set of unsafe states is recursive (although this is generally the case in practice), nor that security in considered Dolev-Yao models is decidable. We rely on existing proof techniques to establish the Dolev-Yao security of protocols (*e.g.* [25, 1, 30, 18, 28, 31, 10, 7, 29, 14, 37]). Sections 3 and 4 aim to extend the scope of these techniques to formal models augmented with a notion of time and probabilities.

3. Transition systems with computation times

In the previous section we have outlined the fact that Dolev-Yao models can be seen as transition systems. In this section, we consider a slightly more complex model

where the transitions are labeled by computation times. These times are functions of a security parameter n, meant to represent the overall strength of the cryptographic schemes, such as the size of the keys.

Formally, a *transition system with computation times* is a triple $T = (Q, q^0, \delta)$ where Q is a countable set of *states*, q^0 is the initial set, and $\delta : \mathbb{N} \times Q \times Q \to [0, \infty]$ is a weight function that maps every $n \in \mathbb{N}$ and every transition to a non-negative real number[3] or to infinity (modeling an impossible transition). Besides we write $q_1 \xrightarrow{f(n)} q_2$ when for all n, $\delta(n, q_1, q_2) = f(n)$. Notice that we do not assume that Q is finite. Practical algorithms dealing with Dolev-Yao models are usually based on some finite representations of such infinite countable graphs.

Having a notion of computational times makes it possible to extend a Dolev-Yao attacker with nonstandard operations. For instance, some nonstandard rules for the example of Section 2 are the following:

- illegitimate decryption: if $\{M\}_K \in E$ then $(q, E) \xrightarrow{f_1(n)} (q, E \cup \{M\})$,
- key guessing: if $\{M\}_K \in E$ (and $M \in E$) then $(q, E) \xrightarrow{f_2(n)} (q, E \cup \{K\})$,
- discrete logarithm: if $e(M) \in E$ then $(q, E) \xrightarrow{f_3(n)} (q, E \cup \{M\})$.

For these nonstandard transitions it is reasonable to assume the time-complexities $f_i(n)$ above to be intractable. We formalize this intuition in the definitions below. Giving a precise, computational justification of the intractability of each corresponding problem would require to detail the concrete implementation and necessary cryptographic assumptions. However, this falls outside the scope of this paper.

Following a standard asymptotic approach we define tractable transitions as those labeled by a polynomially-bounded (in short, polynomial) function of n.

Definition 1 $q_1 \xrightarrow{f(n)} q_2$ *is called* tractable *if* $f(n)$ *is polynomial, or equivalently if* $\frac{\log f(n)}{\log n}$ $(n \geq 2)$ *is bounded from above.*

Clearly enough, defining intractability as the negation of tractability is not sufficient for security purposes. Such a definition would not eliminate *e.g.* cryptographic primitives that are breakable for even values of n but secure for odd values. For this reason, intractable transitions has to be defined in a stricter way.

Definition 2 $q_1 \xrightarrow{f(n)} q_2$ *is called* intractable *if* $\frac{1}{f(n)}$ *is a* negligible *function of* n*, that is* $\lim_{n\to\infty} \frac{\log f(n)}{\log n} = \infty$.

We now define the set of states that can be reached in polynomial time from the initial state. To do so, we define the n-duration of a path $\gamma : q_0 \xrightarrow{f_1(n)} q_1 \xrightarrow{f_2(n)} \ldots \xrightarrow{f_p(n)} q_p$ as the sum of its internal durations:

$$|\gamma|_n = \sum_{i=1}^{p} f_i(n)$$

[3]Duration 0 is allowed although it has arguably no physical meaning. We let $\log(0) = -\infty$.

The n-time cost of a state q is the greatest lower bound of the durations of the paths γ going from the initial state q^0 to q:

$$|q|_n = \inf\{|\gamma|_n, \gamma : q^0 \to \ldots \to q\}$$

Finally we will say that a state q can be reached in polynomial time if $|q|_n$ is polynomial.

Security is defined as the fact that all polynomially-reachable states satisfy a given security property. The question at this point is whether or not the security of our extended model reduces to the security of the underlying standard Dolev-Yao model, obtained by removing intractable transitions, then ignoring computation time altogether.

3.1. Reduction theorem for finite graphs

We start proving a reduction theorem in the case of finite transition systems.

Proposition 3 *Let $T = (Q, q^0, \delta)$ be a transition system with computation times such that Q is finite. Assume that every transition is either tractable or intractable. Then a state q is reachable in polynomial time if and only if there exists a path $\gamma : q^0 = q_0 \xrightarrow{f_1(n)} q_1 \xrightarrow{f_2(n)} \ldots \xrightarrow{f_p(n)} q_p = q$ such that every $f_i(n)$ $(1 \leq i \leq p)$ is polynomial in n.*

The interpretation of this proposition is that extending a (finite) Dolev-Yao model with nonstandard but intractable transitions does not change the set of tractably reachable states. Thus both systems are equivalent as far as security is concerned. The proof is easy; yet we give it in detail so as to emphasize where the finiteness assumption is used.

Proof. The right-to-left implication is clear. Let us consider a state q such that $|q|_n$ is polynomially bounded: let $M > 0$ be such that $\forall n \geq 2$, $|q|_n \leq n^M$.

For each intractable transition $q_1 \xrightarrow{f(n)} q_2$, by definition there exists a n_0 such that $\forall n \geq n_0, f(n) \geq n^{M+1}$. Recall that Q is finite, so the number of intractable transitions is finite. Therefore for $n_0 \geq 2$ large enough, the previous inequality holds for *every* intractable transition at the same time.

Now suppose that every path γ from q^0 to q contains at least one intractable transition. Since weights are positive, this would imply for all $n \geq n_0$, for all such γ, $|\gamma|_n \geq n^{M+1}$. Thus $|q|_n \geq n^{M+1} > n^M$. Contradiction. □

3.2. Reduction theorem for infinite graphs

We now extend the previous result to the infinite case. Some care must be taken because the existence of a uniform value n_0 of n in the previous proof is not guaranteed: we may have an infinite sequence γ_0, γ_1,..., γ_k, ...of paths from q_0 to q such that each $|\gamma_k|_n$ is null for $n \leq k$, which implies $|q|_n = 0$ for all n, and yet for all k, $\lim_{n\to\infty} \frac{\log |\gamma_k|_n}{\log n} = \infty$.

Fortunately this case is unlikely to happen for our purpose. Recall that intractable transitions model some new nonstandard rules in the Dolev-Yao approach. Although rules may have infinitely many instances (*e.g.* sending M over the network would be implemented by as many "send" transitions as there are possible messages, and messages are terms in Dolev-Yao models, of which there are infinitely many), most likely a finite number of rules is applied to a finite number of cryptographic primitives. For that reason, intractable transitions in practice are labeled by (copies of) a finite number of time functions $f_i(n)$. Therefore we can assume that the intractable transitions of the system are *uniformly intractable* in the following sense.

Definition 4 *We say that a system satisfies the* uniform intractability assumption *if for each $M > 0$, there exists a n_0 such that for every intractable transition $q_1 \xrightarrow{f(n)} q_2$, we have $\forall n \geq n_0, \frac{\log f(n)}{\log n} \geq M$.*

Under this assumption, the same proof as before now provides the expected generalization of the reduction theorem.

Proposition 5 *Let $T = (Q, q^0, \delta)$ be a transition system with computation times. Assume that every transition is either tractable or intractable and that the uniform intractability assumption holds. Then a state q is reachable in polynomial time if and only if there exists a path $\gamma : q^0 = q_0 \xrightarrow{f_1(n)} q_1 \xrightarrow{f_2(n)} \dots \xrightarrow{f_p(n)} q_p = q$ such that every $f_i(n)$ $(1 \leq i \leq p)$ is polynomial in n.*

4. Transition systems with probabilistic computation times

In the previous section, we have shown how to account for intractable operations in Dolev-Yao models with deterministic computation times. In practice yet, algorithms may be probabilistic, and it is more relevant to consider the class of tractable problems to be random polynomial-time rather than polynomial-time. By random polynomial-time algorithm we mean here a polynomial-time algorithm using a random oracle, which succeeds (gives a correct result) with a probability at least $\frac{1}{2}$ and fails (gives no result) otherwise. This definition corresponds to the so-called Las Vegas algorithms (see *e.g.* [32]).

As we have been interested in durations previously, it is more natural to state this class in terms of computation time, using the following characterization.

Proposition 6 *Let X be a set of inputs x equipped with a* size function *$\alpha : X \to \mathbb{N}$. Assume that α is computable in polynomial time (*w.r.t. *its result $\alpha(x)$) and for every n, only finitely many inputs may have size n. A computational problem $\mathcal{P}(x)$ admits a Las Vegas algorithm if and only if there exists an algorithm A which always succeeds in giving an answer to $\mathcal{P}(x)$ within probabilistic time $F(\alpha(x))$ and such that*

$$\exists M > 0, \exists N > 0, \exists n_0, \forall n \geq n_0, \mathbb{P}\left(F(n) \leq n^M\right) \geq n^{-N}.$$

Proof. The left-to-right implication is clear. Assume that $\mathcal{P}(x)$ admits an algorithm A satisfying the given property for certain $M > 0$, $N > 0$ and n_0:

$$\forall n \geq n_0, \mathbb{P}\left(F(n) \leq n^M\right) \geq n^{-N}$$

We build a Las Vegas algorithm A' parameterized by $n_1 \geq n_0$ and by a polynomial function $f(n)$ as follows:

- let $n = \alpha(x)$;
- if $n < n_1$, return the correct pre-computed answer (only finitely many inputs have a size less than n_1);
- if $n \geq n_1$, execute A on the entry during at most n^M steps, repeat the execution at most $f(n)$ times, or until success.

By construction A' is polynomial-time and succeeds at least with probability

$$\rho_n = 1 - \left(1 - \mathbb{P}\left(F(n) \leq n^M\right)\right)^{f(n)+1} \geq 1 - \left(1 - n^{-N}\right)^{f(n)+1}.$$

Using the log function, we see that $\rho_n \to 1$ if $\frac{f(n)+1}{n^N} \to \infty$. We conclude by choosing $f(n) = n^{N+1}$ and n_1 big enough such that $\forall n \geq n_1, \rho_n \geq \frac{1}{2}$. □

4.1. The probabilistic model

We now extend our previous model with probabilities. A *transition system with probabilistic computation times* is a triple $T = (Q, q^0, \delta)$ as before but where the values of the weight function $\delta(n, q_1, q_2)$ are independent random variables over some probabilistic space $(\Omega, \mathcal{A}, \mathbb{P})$.[4] We write $q_1 \xrightarrow{F(n)} q_2$ when $F(n)$ is the random variable such that, for all drawing of lots, $\delta(n, q_1, q_2) = F(n)$.

There remains to define a suitable notion of security. Intuitively a system is secure if for every attacker the probability to reach an unsafe state within a polynomial time is negligible. More precisely let P be a security property, that is the choice of a subset $Q_P \subseteq Q$ of *safe states*. In order to define a suitable notion of reachability, we consider for every fixed $n \in \mathbb{N}$ and $t_0 \geq 0$ a $1\frac{1}{2}$-player game between the attacker and a probabilistic opponent. Such probabilistic nondeterministic systems are also known as Markov decision processes (see *e.g.* [34]). The game $G(Q_P, n, t_0)$ is set up as follows:

- the attacker begins in the state q^0 with a time zero;
- let q be the attacker's state and t the time at the beginning of a turn:
  - if $t \leq t_0$ and $q \notin Q_P$ the attacker wins,
  - otherwise the attacker (possibly randomly) chooses a transition $q \xrightarrow{F(n)} q'$ from its current state; the actual value d of $F(n)$ is drawn; the attacker then moves to state q and at time $t + d$.

[4] This means that $\delta(n, q_1, q_2)$ is implicitly a (measurable) function of the drawing of lots $\omega \in \Omega$.

The goal of the attacker is to reach the set of unsafe states within a fixed amount of time with the highest probability. Since durations are positive numbers, paths that contain cycles are useless (cycles do nothing but increase the clock). Thus we only consider strategies of the attacker described by a function $\sigma : Q \times [0, \infty] \times Q \to [0, 1]$ which, given a current state q and a clock t, returns the probability $\sigma(q, t, q')$ of choosing q' as the next state. We write $\mathbb{P}(G_\sigma(Q_P, n, t_0))$ for the probability of a strategy σ to win in the game $G(Q_P, n, t_0)$.

Definition 7 *We will say that P is* verified against every random polynomial attacker *if the probability to reach the unsafe states $Q - Q_P$ within a polynomial time is negligible for every strategy:*

$$\forall M > 0, \forall N > 0, \exists n_0, \forall n \geq n_0, \forall \sigma, \mathbb{P}(G_\sigma(Q_P, n, n^M)) \leq n^{-N}$$

To state our reduction theorem, there remains to define tractable and intractable transitions. To capture the notion of Las Vegas computability, we define tractability as suggested by Proposition 6.

Definition 8 $q_1 \xrightarrow{F(n)} q_2$ *is called* tractable *if it holds that*

$$\exists M > 0, \exists N > 0, \exists n_0, \forall n \geq n_0, \mathbb{P}\left(F(n) \leq n^M\right) \geq n^{-N}.$$

For the same reason as before, intractability has to be stated in a stronger way than just by negating tractability:

Definition 9 $q_1 \xrightarrow{F(n)} q_2$ *is called* intractable *if it holds that*

$$\forall M > 0, \forall N > 0, \exists n_0, \forall n \geq n_0, \mathbb{P}\left(F(n) \leq n^M\right) \leq n^{-N}.$$

This definition is satisfactory as it matches the classical definitions of cryptographic security that require the probability of *e.g.* successfully inverting a one-way function in probabilistic non-polynomial time to be *negligible*. For infinite systems, as in the deterministic case, we have to introduce the notion of *uniform intractability* and require the n_0 above to be chosen uniformly over the intractable transitions.

Definition 10 *We say that the* uniform intractability assumption *holds if*

$$\forall M > 0, \forall N > 0, \exists n_0, \forall n \geq n_0, \forall q_1 \xrightarrow{F(n)} q_2 \text{ intractable}, \mathbb{P}\left(F(n) \leq n^M\right) \leq n^{-N}.$$

Again this assumption is satisfied in our case because a finite number of nonstandard rules and cryptographic primitives is used (see Section 3.2).

4.2. Reduction theorem for infinite probabilistic graphs

We can now state the corresponding reduction theorem:

Theorem 11 *Let $T = (Q, q^0, \delta)$ be a transition system with probabilistic computation times and P be a security property. Assume that every transition is either tractable or intractable and that the uniform intractability assumption holds. Then P is verified against every random polynomial attacker if and only if there exists no path $\gamma : q^0 = q_0 \xrightarrow{F_1(n)} q_1 \xrightarrow{F_2(n)} \dots \xrightarrow{F_p(n)} q_p = q$ such that every $F_i(n)$ $(1 \leq i \leq p)$ is tractable and $q \notin Q_P$.*

Proof. The left-to-right implication is obvious (if there exists such a polynomial path, one can define a strategy that follows it). Suppose that P is not verified: there exists $M > 0$ and $N > 0$ such that $\forall n_0, \exists n \geq n_0, \exists \sigma,\ \mathbb{P}(G_\sigma(Q_P, n, n^M)) > n^{-N}$. From the intractability assumption, we deduce that there exist n and σ such that $\mathbb{P}(G_\sigma(Q_P, n, n^M)) > n^{-N}$ and for every intractable transition $q_1 \xrightarrow{F(n)} q_2$, $\mathbb{P}\left(F(n) \leq n^M\right) \leq n^{-N}$.

Before we proceed we need to express the probability $\mathbb{P}(G_\sigma(Q_P, n, n^M))$ in a more precise way. Let $p(q, t, k)$ be the probability for σ to win in the current game from the state q and the time t in at most k steps ($k \geq 0$). Using the fact that the drawings are independent from each other, the definition of games and strategies σ implies that

- $p(q, t, k) = 1$ if $t \leq n^M$ and $q \notin Q_P$,
- otherwise, $p(q, t, 0) = 0$ and the probability to win in $(k+1)$ steps can be written as a sum of the probability to win in k steps conditioned by the choice of the attacker and the drawing of the next duration:

$$p(q, t, k+1) = \sum_{q \xrightarrow{F(n)} q'} \sigma(q, t, q') \int_\Omega p(q', t + F(n)(\omega), k)\ d\mathbb{P}(\omega) \tag{4.1}$$

Now we can rewrite the probability of success as

$$\mathbb{P}(G_\sigma(Q_P, n, n^M)) = \sup_{k \in \mathbb{N}} p(q^0, 0, k).$$

Since $p(q^0, 0, k)$ is monotone in k, the hypothesis implies that there exists a k_0 such that $p(q^0, 0, k_0) > n^{-N}$. We prove the auxiliary lemma:

Lemma 12 *For all q, t, k such that $p(q, t, k) > n^{-N}$, there exists a path starting from q, leading to a state $q' \notin Q_P$, and of which every transition $q_1 \xrightarrow{F(n)} q_2$ satisfies (i) $\mathbb{P}(F(n) \leq n^M) > n^{-N}$.*

We conclude by applying the lemma to $p(q^0, 0, k_0) > n^{-N}$ and noticing that condition (i) on the transitions of the path implies that all these are intractable.

We now proceed and prove the auxiliary lemma by induction on k. If $q \notin Q_P$, simply consider the empty path from q. Otherwise ($q \in Q_P$), first notice that $p(q, t, k) > 0$ implies $t \leq n^M$ and $k = k'+1 > 0$. Now consider Eq. (4.1) for $p(q, t, k'+1)$. This quantity is greater than n^{-M} by assumption. By definition of σ, we have $\sum_{q'} \sigma(q, t, q') = 1$. Thus for the inequality to hold, we must have for some transition $q \xrightarrow{F(n)} q'$,

$$\int_\Omega p(q', t + F(n)(\omega), k')\ d\mathbb{P}(\omega) > n^{-N}.$$

But since $p(q, t, k') = 0$ whenever $t > n^M$, this integral is also bounded from above by

$$\left(\sup_{t' \geq t} p(q', t', k')\right) \mathbb{P}\left(F(n) \leq n^M\right).$$

As the two factors are not greater than 1, they must be both greater than n^{-N}. In particular there exists $t' \geq t$, such that $p(q', t', k') > n^{-N}$. We conclude by applying the induction hypothesis on q', t', k'. □

5. Conclusion

A recent and important trend in security protocol verification [3, 2, 22, 12, 21, 6, 24, 26, 5, 20, 27, 13, 35] is to relate the computational models of security, based on networks of probabilistic polynomial-time Turing machines, and the formal ones, based on ideas originating from Dolev and Yao [16].

In this work, we followed a different approach, initiated by Zunino and Degano [39], and tried to answer the question: how much do Dolev-Yao style models really prove? We first noticed that, from a sufficiently abstract perspective, Dolev-Yao style models were just transition systems, possibly infinite. Extending these transition systems with computation times and probabilities is natural and makes it possible to account for nonstandard transitions such as guessing a key or inverting a hash function. Informally, our main contribution is to show that, if there is any attack in the latter, extended model, then some unsafe state was already reachable in the initial Dolev-Yao model, where only tractable transitions are kept. Compared to previous work [39], our more general setting allowed us to state our result for a large class of Dolev-Yao models. We also added a notion of computation time and emphasized the role of the so-called uniform intractability assumption in proofs.

Our approach applies to any security property that can be expressed as random polynomial-time (Las Vegas) unreachability. This includes secrecy, various forms of authentication [4], but also more sophisticated requirements, such as those found in e-commerce protocols [11]. An interesting avenue is whether this can be extended to more complex properties, not expressible by reachability, such as those used in fair contract signing [19], which cannot even be expressed in say, linear time temporal logic, but profit from game semantics.

Acknowledgments

We are grateful to Jean Goubault-Larrecq and Florent Jacquemard for comments on earlier versions of the paper, to Thierry Cachat and Stéphane Messika for interesting talks about probabilistic games.

References

[1] M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: The Spi calculus. In: *Proc. 4th ACM Conference on Computer and Communications Security (CCS'97)*, (1997), 36–47.

[2] M. Abadi and J. Jürjens. Formal eavesdropping and its computational interpretation. In: *Proc. 4th International Symposium on Theoritical Aspects of Computer Software (TACS'01)*, LNCS **2215** (2001), 82–94.

[3] M. Abadi and P. Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). In: *Proc. 1st IFIP International Conference on Theoretical Computer Science (IFIP–TCS'00)*, LNCS **1872** (2000), 3–22.

[4] R. M. Amadio and D. Lugiez. On the reachability problem in cryptographic protocols. In: *Proc. 11th International Conference on Concurrency Theory (CONCUR'00)*, LNCS **1877** (2000), 380–394.

[5] M. Backes and B. Pfitzmann. Symmetric encryption in a simulatable Dolev-Yao style cryptographic library. In: *Proc. 17th IEEE Computer Science Foundations Workshop (CSFW'04)*, (2004), 204–218.

[6] M. Backes, B. Pfitzmann, and M. Waidner. A composable cryptographic library with nested operations. In: *Proc. 10th ACM Conference on Computer and Communications Security (CCS'03)*, (2003), 220–230.

[7] B. Blanchet. An efficient cryptographic protocol verifier based on Prolog rules. In: *Proc. 14th IEEE Computer Security Foundations Workshop (CSFW'01)*, (2001), 82–96.

[8] B. Blanchet. From secrecy to authenticity in security protocols. In: *Proc. 9th International Static Analysis Symposium (SAS'02)*, LNCS **2477** (2002), 342–359.

[9] C. Bodei, M. Buchholtz, P. Degano, F. Nielson, and H. R. Nielson. Automatic validation of protocol narration. In: *Proc. 16th IEEE Computer Security Foundations Workshop (CSFW'03)*, (2003), 126–140.

[10] C. Bodei, P. Degano, F. Nielson, and H. R. Nielson. Flow logic for Dolev-Yao secrecy in cryptographic processes. *Future Generation of Computer Systems* **18** (2002) 6, 747–756.

[11] D. Bolignano. Towards the formal verification of electronic commerce protocols. In: *Proc. 10th IEEE Computer Security Foundations Workshop (CSFW'97)*, (1997), 113–147.

[12] R. Canetti. Universally composable security: A paradigm for cryptographic protocols (extended abstract). In: *Proc. 42nd IEEE Symposium on Foundations of Computer Science (FOCS'01)*, (2001), 136–147.

[13] R. Canetti. Universally composable signature, certification, and authentication. In: *Proc. 17th IEEE Computer Security Foundations Workshop (CSFW'04)*, (2004), 219–235.

[14] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the security of protocols with Diffie-Hellman exponentiation and products in exponents. In: *Proc. 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FST–TCS'03)*, LNCS **2914** (2003), 124–135.

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

[16] D. Dolev and A. C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory* **IT-29** (1983) 12, 198–208.

[17] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences* **28** (1984), 270–299.

[18] A. Huima. Efficient infinite-state analysis of security protocols. In: *Proc. FLOC Workshop on Formal Methods and Security Protocols*, (1999).

[19] S. Kremer and J.-F. Raskin. Game analysis of abuse-free contract signing. In: *Proc. 15th IEEE Computer Security Foundations Workshop (CSFW'02)*, (2002), 206–222.

[20] P. Laud. Symmetric encryption in automatic analyses for confidentiality against active adversaries. In: *Proc. IEEE Symposium on Security and Privacy (SSP'04)*, (2004), 71–85.

[21] P. Laud and R. Corin. Sound computational interpretation of formal encryption with composed keys. In: *Proc. 6th International Conference on Information Security and Cryptology (ICISC'03)*. KIISC (2003).

[22] P. Lincoln, J. C. Mitchell, M. Mitchell, and A. Scedrov. A probabilistic poly-time framework for protocol analysis. In: *Proc. 5th ACM Conference on Computer and Communications Security (CCS'98)*, (1998), 112–121.

[23] G. Lowe. An attack on the Needham-Schroeder public-key authentication protocol. *Information Processing Letters* **56** (1995) 3, 131–133.

[24] P. Mateus, J. C. Mitchell, and A. Scedrov. Composition of cryptographic protocols in a probabilistic polynomial-time process calculus. In: *Proc. 14th International Conference on Concurrency Theory (CONCUR'03)*, LNCS **2761** (2003), 323–345.

[25] C. Meadows. The NRL protocol analyzer: An overview. *Journal of Logic Programming* **26** (1996) 2, 113–131.

[26] D. Micciancio and B. Warinschi. Completeness theorems for the Abadi-Rogaway logic of encrypted expressions. *Journal of Computer Security* **12** (2004) 1, 99–129.

[27] D. Micciancio and B. Warinschi. Soundness of formal encryption in the presence of active adversaries. In: *Proc. 1st Theory of Cryptography Conference (TCC'04)*, LNCS **2951** (2004), 133–151.

[28] J. K. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In: *Proc. 8th ACM Conference on Computer and Communications Security (CCS'01)*, (2001), 166–175.

[29] J. K. Millen and V. Shmatikov. Symbolic protocol analysis with products and Diffie-Hellman exponentiation. In: *Proc. 16th IEEE Computer Security Foundations Workshop (CSFW'03)*, (2003), 47–61.

[30] J. C. Mitchell, M. Mitchell, and U. Stern. Automated analysis of cryptographic protocols using Murϕ. In: *Proc. IEEE Symposium on Security and Privacy (SSP'97)*, (1997) 141–153.

[31] D. Monniaux. Abstracting cryptographic protocols with tree automata. *Science of Computer Programming* **47** (2003) 2–3, 177–202.

[32] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.

[33] O. Pereira and J.-J. Quisquater. Security analysis of the Cliques protocols suites. In: *Proc 14th IEEE Computer Security Foundations Workshop (CSFW'02)*, (2001), 73–81.

[34] M. L. Puterman. *Markov Decison Processes: Discrete Stochastic Dynamic Programming*. John Wiley & Sons, 1994.

[35] A. Ramanathan, J. C. Mitchell, A. Scedrov, and V. Teague. Probabilistic bisimulation and equivalence for security analysis of network protocols. In: *Proc. 7th International Conference on Foundations of Software Science and Computation Structures (FOSSACS'04)*, LNCS **2987** (2004), 468–483.

[36] M. Roger. *Raffinements de la résolution et vérification de protocoles cryptographiques*. PhD thesis, ENS Cachan, 2003.

[37] K. N. Verma. Two-way equational tree automata for AC-like theories: decidability and closure properties. In: *Proc. 14th International Conference on Rewriting Techniques and Applications (RTA'03)*, LNCS **2706** (2003), 180–196.

[38] B. Warinschi. A computational analysis of the Needham-Schroeder protocol. In: *Proc. 16th IEEE Computer Science Foundations Workshop (CSFW'03)*, (2003), 248–262.

[39] R. Zunino and P. Degano. A note on the perfect encryption assumption. In: *Proc. 7th International Conference on Foundations of Software Science and Computation Structures (FOSSACS'04)*, LNCS **2987** (2004), 514–528.