Improving Automatic Verification of Security Protocols with XOR

Xihui Chen¹,², Ton van Deursen¹,* and Jun Pang¹

¹ Faculty of Sciences, Technology and Communication
University of Luxembourg, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg
² School of Computer Science and Technology
Shandong University, Jinan, 250101 China

Abstract. Küsters and Truderung recently proposed an automatic verification method for security protocols with exclusive or (XOR). Their method reduces protocols with XOR to their XOR-free equivalents, enabling efficient verification by tools such as ProVerif. Although the proposed method works efficiently for verifying secrecy, verification of authentication properties is inefficient and sometimes impossible.

In this paper, we improve the work by Küsters and Truderung in two ways. First, we extend their method for authentication verification to a richer class of XOR-protocols by automatically introducing bounded verification. Second, we improve the efficiency of their approach by developing a number of dedicated optimizations. We show the applicability of our work by implementing a prototype and applying it to both existing benchmarks and RFID protocols. The experiments show promising results and uncover a flaw in a recently proposed RFID protocol.

1 Introduction

Cryptographic security protocols typically consist of a series of message exchanges among two or more agents over a hostile network. They aim to achieve various security goals such as authentication, secrecy, key agreement, privacy, and anonymity. However, designing secure protocols is an error-prone task and incorrect protocols may become ideal entry points for various attacks. Starting from the seminal work by Lowe [1], automated symbolic verification methods for security protocols have shown their strength in finding attacks and proving correctness of security protocols.

As attacks that rely on cryptographic primitives are hard to prove and difficult to be automatically checked, cryptographic primitives are usually treated as functions without any algebraic properties in symbolic methods. This is called the perfect cryptography assumption [2], namely no cryptographic message can be opened without the correct key. Based on this assumption, many automatic tools have been designed and implemented, among which ProVerif [3] is considered as the state of the art [4]. However, ProVerif cannot uncover attacks that

* Ton van Deursen was supported by a grant from the Fonds National de la Recherche (Luxembourg).
make use of certain algebraic properties of cryptographic primitives. Cortier, Delaune and Lafourcade give a survey on algebraic properties of common cryptographic primitives and attacks making use of them [5]. Therefore, some relaxation of the perfect assumption needs to be investigated. Exclusive or (XOR) is one binary operator with typical algebraic properties that has drawn a lot of interest. For example, XOR is often used in radio frequency identification (RFID) systems, which have become popular in recent years.

We call security protocols employing the exclusive or operator \((\oplus)\) XOR-protocols. The \(\oplus\)-operator has the following four properties.

\[
\begin{align*}
  x \oplus (y \oplus z) &= (x \oplus y) \oplus z & \text{(associativity)} & (1) \\
  x \oplus y &= y \oplus x & \text{(commutativity)} & (2) \\
  x \oplus 0 &= x & \text{(neutral element)} & (3) \\
  x \oplus x &= 0 & \text{(nilpotence)} & (4)
\end{align*}
\]

In order to detect attacks on XOR-protocols, we need to model intruders with the ability of exploring the above algebraic properties, in addition to the perfect cryptography assumption.

Related work. In the literature, several approaches have been proposed to deal with the verification of XOR-protocols [6,7,8], but few of them are practical to implement. A few tools can cope with a certain class of XOR-protocols [8,9], all of them have strict restrictions on the range of protocols they can be applied to. For example, the tool of Cortier, Keighren, and Steel can only handle protocols with the \(\oplus\)-operator and symmetric encryption. More recently, Küsters and Truderung proposed a more general approach [10] to automatic verification of cryptographic XOR-protocols based on ProVerif. Their main idea is to reduce protocol analysis with XOR to the XOR-free case. The XOR-reduction step transforms Horn theories modeling XOR-protocols to the ones free from algebraic properties of the \(\oplus\)-operator, by computing a family of legal substitutions for terms containing \(\oplus\). Thus, verification is reduced to a syntactic derivation problem. They implement their transformation step in a tool called XorProverif [10]. The use of ProVerif allows the modeling of essential cryptographic primitives and the verification of security protocols with an unbounded number of sessions. However, there are still a few limitations of this XOR-reduction approach – only \(\oplus\)-linear protocols can be handled (see Sect. 2 for the definition of \(\oplus\)-linearity) and it is likely to suffer from exponential blow up of the number of substitutions (Lem. 12, [10]).

In this paper, we develop several methods to tackle these restrictions of the XOR-reduction approach, and implement a prototype to evaluate and illustrate our methods by experiments on existing benchmarks and recent RFID protocols.

Our main contribution. One goal of this research is to develop a systematic method to improve efficiency of the XOR-reduction approach. Our first idea is to reduce the number of substitutions during the transformation, by exploring the freshness of nonces generated during the executions of the XOR-protocols. By this further reduction, the time taken by ProVerif for verification is decreased and some false attacks can be removed as well.