Addressing New Challenges by Building Security Protocols Around Graphs

Kamil Kulesza and Zbigniew Kotulski

Computer Science Department,
Institute of Fundamental Technological Research,
Polish Academy of Sciences,
ul.Świętokrzyska 21, 00-049, Warsaw, Poland
{kkulesza, zkotulsk}@ippt.gov.pl

Abstract. We propose the use of graphs as basic objects in security protocols. While having all the functionality of their number based counterparts; such protocols can have extended capabilities, especially useful in the field of verification and analysis. The scalability and transitivity for graph related properties allow for addressing protocols of increasing complexity. These features also cater for new challenges in the future, for instance ones resulting from a quantum computing paradigm.

Keywords: security protocols, data security, graph theory, secret sharing, graph colouring, extended capabilities, quantum computing.

1 Introduction

The main goal of this paper is to stimulate discussion on alternatives in security protocol design, which should have a great effect on protocol analysis and verification.

When it comes to cryptology, number theory is king, as it underlies the majority of cryptographic algorithms and protocols. Claude Shannon, in his fundamental Mathematical Theory of Communication ([1]), introduced a description of information as a string of bits. Usually a bit string has been thought of as a binary number. Binary numbers are easy to manipulate, hence this approach underlies virtually all modern computing. Yet, theoretically speaking, binary strings can also represent other objects, like graphs. When they are used to describe the structure of a graph, they actually contain much more information than only about the structure.

In order to benefit from this observation one needs to make practical use of the surplus information. One possibility is to use a conversion between graphs and numbers, for example methods based on Goedel's numbering ([2]). There are other numerous ways to do so (see [3], [4]). When some additional conditions are met, such conversion allows one to use traditional, number theory based cryptographic methods, while also gaining the advantage from graph embedded information. Such opportunity is especially interesting taking into account connections between graph theory and other branches of mathematics like: coding theory, topology and knot theory (see [5]).

B. Christianson et al. (Eds.): Security Protocols 2003, LNCS 3364, pp. 301–306, 2005.

Graph theory provides us with a variety of interesting problems, many of which are known to be of NP class (*e.g.*, [3]). Examples are: graph colouring, graph isomorphism and Hamiltonian paths, all of which can be used to provide extended capabilities for security protocols.

One should remember that problems from the same complexity class can be used interchangeably, at least in the graph case. Very good examples are zero-knowledge proofs, that were designed independently for various graph problems, for instance isomorphism (*e.g.*, [6]) and colouring (*e.g.*, [7]). In [6], Goldreich *et al.* have shown that any NP-complete problem can be turned into a zero-knowledge proof. Hence, the choice of problem to work with is only a matter of individual taste.

On the other hand, the above mentioned problems are handy when it comes to the issue of provable security (*e.g.*, [8], [9]). In this paper we wish to concentrate on the most promising field: verification and analysis of the protocols in the provable security context.

In security protocols the role of the graphs has mainly been limited to modelling the data structures. Although significant results have been obtained, with the proposed approach we hope to go much further.

The goal of this paper is to discuss the advantages of using graphs as the building blocks for security protocols. In Section 2 we briefly describe an example of graph colouring based verifiable secret sharing (VSS). Section 3 is meant to stimulate discussion on the interactions between graph object(s) that underlie the protocol and graph based data models. At the outset we outline two graph related properties: scalability and transitivity. Next, we discuss how they can be applied to handle increasing protocol complexity. At the end of the section, we briefly refer to problems resulting from quantum computing methods. The conclusions are provided in Section 4.

2 Graph Colouring Based Verifiable Secret Sharing

In this section an illustrative example, from research into Verifiable Secret Sharing, will be presented. First, we provide some background information on secret sharing.

Everybody knows situations, where permission to trigger certain action requires approval of several selected entities. Equally important is that any other set of entities cannot trigger the action. Secret sharing allows a secret to be split into different pieces, called shares, which are given to the participants, such that only certain groups (authorized sets of participants) can recover the secret.

The access structure is the set of all authorized subsets of participants. Good general references for secret sharing are the books by Stinson [10] and by Pieprzyk *et al.* [11]; an interested reader can also consult the bibliography list by Stinson [12].

Once secret sharing was introduced, it was found that it can be easily compromised by misbehaving parties. Hence, the ability to perform secret consistency verification and detection of cheaters is very important. One of solutions is to

use Verifiable Secret Sharing (VSS). The verification capacity usually comes at a price. This fact is related to the paradox stated by David Chaum, that no system can simultaneously provide privacy and integrity.

At ESORICS2002 in Zurich, a verification method that works for any underlying secret sharing scheme was described ([13]). It is based on the concept of verification sets of participants, related to an authorized set of participants. The participants interact (with no third party involvement) in order to check validity of their shares, before they are pooled for secret recovery. Verification efficiency does not depend on the number of faulty participants. One of the pillars of the method is the use of a proper verification function; a very promising one results from the graph colouring check-digit scheme described in [14]. This proposal requires conversion of the given number into a graph and checking its vertex colouring on both sides of the communication channel. The quantitative argument presented shows that the feasibility of the proposed scheme increases with the size of the number whose digits are checked, as well as, overall probability of digits errors.

Joining both results ([13], [14]) produces a graph-based shares verification method. The method depends heavily on graph colouring properties that in turn are handy in the formal security analysis. To some extent it seems even to bypass (or at least weaken) the Chaum paradox. In the case of described method one does not get a free lunch, but at least can have a free starter.

3 Advantages of Graph Based Security Protocols

Before entering into a discussion of what graphs can do for security protocols, we need to outline two graph related properties:

a. Scalability. The fastest informal description is that the level of complication in a graph increases exponentially with the number of vertices, while testing for basic graph properties can be usually done in polynomial time. Very good instances are bounds on chromatic numbers (*e.g.*, [3], [15]).

Example 1.
Definitions:
The degree of vertex in the graph is the number of edges connected to that vertex.

The complete graph is the graph, such that every vertex is linked with all remaining vertices.

The odd cycle is a connected graph, having odd number of vertices, with each vertex having degree equal to 2.

Theorem by Brooks (1941): Let G be a connected graph. If G is neither complete nor an odd cycle, then its chromatic number is smaller or equal to the maximum degree of vertex in G. •

Scalability is used in the graph colouring check-digit scheme (see [14]). It also works well in formal analysis of access structures in secret sharing

protocols. If the graph representing an access structure belongs to some instance graph theoretical class, specified information theoretical properties of the secret sharing method are conserved (*e.g.*, [10]).

b. Transitivity (proliferation). Given any graph, even a small alteration made to the structure (or the way the graph property is described), may have far reaching consequences. This can be understood figuratively and literally – resulting changes can pop up far away in the graph. Again, graph colouring is a very good example. Even a single vertex or edge modification made to the structure can dramatically change colouring (for an example see [4]). On the other hand, for a given colouring of a graph, alteration of one vertex colour can proliferate through an entire system (*e.g.*, [4]).

By its nature, scalability is very useful when managing complexity. This may even start at the protocol design stage. The example given in the Section 2 falls into this category. In this case, the access structure design can be refined, until it represents the best quality in the information theoretical meaning. We present an example coming from the book by Stinson ([10]).

Example 2.
Let's denote:
E as set of edges for the given graph G;
V as set of vertices for the given graph G;
$cl(E)$ as the closure on the set E.
Definitions:
The complete multipartite graph, such that vertices can be partitioned in the finite number of disjoined sets such that:

a. vertices in one set are not linked be the edge;
b. each vertex is linked with all the vertices outside the set.

A secret sharing scheme is ideal if its information rate is 1, so the length of the secret equals to the length of a share held by a participant. The information rate is defined in the Shannon sense (see [1]).

Theorem: Suppose G is a complete multipartite graph. Then there is an ideal scheme realizing the access structure $cl(E)$ on participant set V. •

Yet, more interesting applications of scalability arise when dealing with analysis and verification of the protocols. When the protocol is a complex collection of the interacting parts (or even protocols), there are two basic techniques: cryptoanalytic and formal. Unfortunately both schools rarely interact (*e.g.*, [16]). Scalability, together with the application of graph based protocols, offers an opportunity to reconcile both approaches to the protocol analysis and verification.

The underlying (graph based) parts would be treated in the cryptoanalytic style, while their interaction would be investigated on a higher level. Both levels of analysis would deal with objects of the same type. Hence, merging them into one, more abstract, construct should be possible. On the other hand, use of scalability would facilitate good information theoretical description of the resulting construct.

The second property addresses the issue of how small changes in one place can have an effect on the whole system. This is a handy add-on for the approach outlined above. Adding transitivity into the picture would address the problem of losing the details when trying to abstract some concepts. This natural process has proven to be dangerous in the analysis of the protocols. The introduction of the transitivity allows for taking care of the details that should not be lost during a shift to higher levels of abstraction. Hence, in the analysis of security protocols, transitivity should be used together with scalability, compensating for its possible weaknesses.

A graph based approach provides capabilities for handling potential problems resulting from quantum computing methods. Once quantum algorithms (or protocols) are embedded into the system, apart from the normal considerations, one should take care about resulting quantum effects, like interference or entanglement (*e.g.*, [17]).

Informally speaking, entanglement means that the properties of a composite (quantum) system, even when the components are distant and non-interacting, are linked. In general they cannot be fully expressed by descriptions of the properties of all the component systems. Hence, the system is more than only the sum of all components.

Transitivity seems to be very well suited, at least partially, to addressing issues resulting from the quantum entanglement. It is noteworthy that the same description as for entanglement fits problems in vertex colouring of the graphs.

4 Conclusions

We advocate using graph based security protocols. They result in the situation where one abstract type simultaneously underlies and models the protocol. This, in turn, allows one to see interaction of the protocol parts in a new light. The example from graph colouring and secrets sharing was used in order to illustrate the proposal, as well as to stimulate the discussion. Nevertheless, the graph theory provides much more opportunities. In general terms the most important is the chance for a unified approach to protocol analysis and verification, and also for the emerging quantum computing paradigm.

We hope that graph based protocols will bring new insight into the way that complex systems interact. Other opportunities arise from investigations into the interactions between graph theory and other branches of mathematics (*e.g.*, [5]).

Acknowledgement

The article was completed during a visit to Rhodes University, Grahamstown, South Africa. The authors wish to thank Prof. Patrick Terry for reading the manuscript and for his critical remarks.

References

1. Shannon C.E.: *A mathematical theory of communication.* Bell System Technical Journal, **27** (1948) 379–423
2. Goedel K.: *Uber formal unentscheidbare Satze der Principia Mathematica und verwander Systeme, I.* Monatshefte fur Mathematik und Physik, **38** (1931) 173–198
3. Korte B., Vygen J.: *Combinatorial Optimization, theory and algorithms.* Springer-Verlag, Berlin Heilderberg New York (2000)
4. Molloy M., Reed B.: *Graph Colouring and the Probabilistic Method.* Springer-Verlag, Berlin Heilderberg New York (2002)
5. Beineke L.W., Wilson R.J. (Eds.): *Graph connections; relationships between graph theory and other areas of mathematics.* Oxford University Press, New York (1997)
6. Goldreich O., Micali S., Wigderson A.: *Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems.* Journal of the ACM, **38**(1) (1991) 691–729
7. Brassard G., Chaum D., and Crepeau C.: *Minimum disclosure proofs of knowledge.* Journal of Computer and System Science, **37**(2) (1988) 156–189
8. Goldwasser S.: *The search for provably secure cryptosystems.* In: Pomerance C. (Ed.): Cryptology and Computational Number Theory, Proceedings of Symposia in Applied Mathematics **42** (1990) 89-113, American Mathematical Society
9. Maurer U.M.: *Information-theoretically secure secret-key agreement by NOT authenticated public discussion.* In: Fumy W. (Ed.) Advances in Cryptology Eurocrypt '97 , LNCS, Vol. 1233, Springer-Verlag, Berlin Heilderberg New York (1997)
10. Stinson D.R.: *Cryptography, Theory and Practice.* CRC Press, Boca Raton (1995)
11. Pieprzyk J., Hardjono T. and Seberry J.: *Fundamentals of Computer Security.* Springer-Verlag, Berlin Heilderberg New York (2003)
12. Stinson D.R., Wei R.: *Bibliography on Secret Sharing Schemes.* Webpage: http://www.cacr.math.uwaterloo.ca/ dstinson/ssbib.html. Retrieved 30.08.2003.
13. Kulesza K., Kotulski Z., Pieprzyk J.: *On alternative approach for verifiable secret sharing.* ESORICS2002, Zurich. Submitted for publication, available from IACR's Cryptology ePrint Archive (http://eprint.iacr.org/) report 2003/035
14. Kulesza K., Kotulski Z.: *On graph coloring check-digit method.* Submitted for publication, available from the Los Alamos National Laborartory e-print (http://arxiv.org/abs/math.CO/0211317) (2002)
15. Wilson R.A.: *Graphs, Colourings and the Four-colour Theorem.* Oxford University Press, New York (2002)
16. Ryan P.: *Open questions.* In: Christianson B. *et al.* (Eds.): Security protocols, LNCS Vol. 2133, 49–53, Springer-Verlag, Berlin Heilderberg New York (2001)
17. Gruska J.: *Quantum Computing.* McGraw Hill, New York (1999)