4-15-2022

Graph Embedded Term Rewrite Systems

Saraid Satterfield

GRAPH-EMBEDDED TERM REWRITE SYSTEMS AND APPLICATIONS

Saraid Dwyer Satterfield[1] **Serdar Erbatur**[2]
Andrew M. Marshall[1] **Christophe Ringeissen**[3]

[1]University of Mary Washington, Fredericksburg, VA, USA
[2]University of Texas at Dallas, Dallas, TX, USA [3]Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

Three Threads of Research Meet

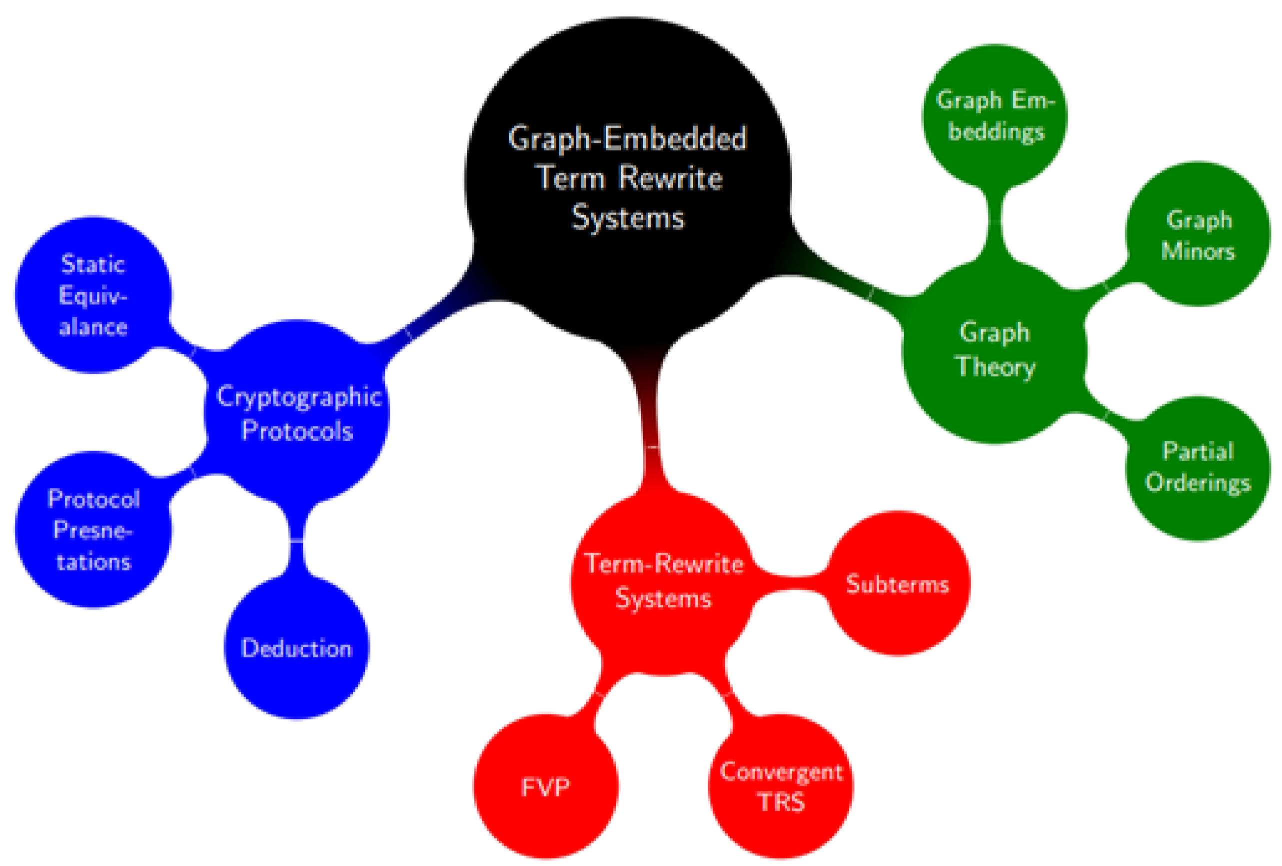

Fig. 1: Threads of Research

The Motivating Question

- We would like to extend the ability of cryptographic protocol analysis tools.
  - Prove security questions about a wider set of cryptographic systems
- Many systems already work for "subterm-convergent" presentations. Many also work for specific examples of protocols that are beyond subterm-convergent.
- However, there is no syntactic definition of this "beyond subterm" or no classification of what systems fit into this class.

Can we define a new form of beyond subterm-convergent Term Rewrite System (TRS) and prove it can be used to extend the ability of existing cryptographic protocol analysis methods?

Multi-Set of Keys

The theory of a multi-set of keys:

$$d(e(x, y), y) \to x$$
$$d(e(x, f(y, z)), y) \to e(x, z)$$
$$d(e(x, y), f(y, z)) \to d(x, z)$$
$$d(e(x, f(y, z)), f(y, v)) \to d(e(x, z), v)$$

Note: The theory of a multi-set of keys is **not** subterm-convergent, yet the procedure of [1] still works. Why?

Road Map

We take the following path to a solution:

- Using notions of graph theory develop a new definition of graph-embedded relation on terms.
- Extend the graph embedded notion on terms to term-rewrite systems.
- Prove that these new "graph-embedded TRS" encompass the required properties of the cryptographic analysis systems.
- Prove that the protocol analysis systems work on the classes of graph-embedded TRS, namely that they have the local stability property.

Graph Theory to Term-Rewrite Systems

Graph Theory to Term-rewrite System: Graph Minor

Definition 1. G is an MG', denoted $G = MG'$, if G' can be obtained from G by a series of edge contractions. That is, iff there exists graphs $G_0, G_1, \ldots, G_n$ and edges $e_i \in G_i$ such that $G = G_0, G_n \simeq G'$, and $G_{i+1} = G_i/e_i$ for all $i < n$.
If $G = MG'$ and G is a subgraph of another graph G'', we call G' a *graph minor* of G'', denoted as $G' \succcurlyeq G''$.

Graph Theory to Term-rewrite System: Graph Embedded Term

Definition 2. Consider the following reduction relation, $\to^*_{R_{gemb}}$, induced by the set of rewrite rules create after instantiating the following rule schema with Σ:

$$R_{gemb} = \{$$
$$(1) f_i(x_1, \ldots, x_n) \to x_i \mid n \geq 1,\ 1 \leq i \leq n$$
$$(2) f_i(x_1, \ldots,\ x_{i-1},\ x_i,\ x_{i+1}\ \ldots,\ x_n) \to f_i(x_1, \ldots,\ x_{i-1},\ x_{i+1},\ \ldots,\ x_n)$$
and $\forall f_i, f_j \in \Sigma$
$$(3) f_i(x_1, \ldots, x_{i-1}, f_j(\bar{z}), x_{i+1},\ \ldots, x_m) \to f_j(x_1, \ldots,\ x_{i-1}, \bar{z}, x_{i+1},\ \ldots, x_m)$$
$$(4) f_i(x_1, \ldots, x_{i-1}, f_j(\bar{z}), x_{i+1},\ \ldots, x_m) \to f_i(x_1, \ldots,\ x_{i-1}, \bar{z}, x_{i+1},\ \ldots, x_m)$$
$$\}$$

We say a term t' is graph embedded in a term t, denoted $t' \succcurlyeq_{gemb} t$, if t' is a well formed term and $t \to^*_{R_{gemb}} s \approx t'$.

Graph Theory to Term-rewrite System: Graph Embedded TRSs

Definition 3. A TRS R is a graph embedded TRS if $\forall\ l \to r \in R,\ r \succcurlyeq_{gemb} l$.

Protocol Analysis

Resulting Theorems

Theorem: Let R be a convergent graph-embedded and cap-contracting TRS. Then, R is locally stable.

Corollary: Let R be a convergent, graph-embedded, and cap-contracting TRS. Then deduction and static equivalence are decidable.

Multi-Set of Keys Using TRS

The theory of a multi-set of keys:

$$d(e(x, y), y) \to x$$
$$d(e(x, f(y, z)), y) \to e(x, z)$$
$$d(e(x, y), f(y, z)) \to d(x, z)$$
$$d(e(x, f(y, z)), f(y, v)) \to d(e(x, z), v)$$

We see the multi-set of keys is not subterm-convergent, yet the procedure of [1] still works. Why? Because the theory is a convergent, graph-embedded, and cap-contracting TRS.

Conclusion

As a result of this research, we have developed a new form of graph-embedded term rewrite system. Additionally, we have proven several properties such as termination and that they differ from homeomorphic embedded systems. These properties were then used to show how graph-embedded term rewrite systems can be used to analyze cryptographic protocols, for example, by using local stability. In future work, we would like to explore more applications for graph-embedded term rewrite systems, as well as investigating if additional embedding properties such as topological embeddings are useful.

Acknowledgements

I would like to thank Dr. Andrew Marshall, Dr. Erbatur, and Dr. Ringeissen for allowing me to join their research team.

References

[1] Martín Abadi and Véronique Cortier. Deciding knowledge in security protocols under equational theories. *Theor. Comput. Sci.*, 367(1-2):2–32, 2006.

[2] Martín Abadi and Cédric Fournet. Mobile values, new names, and secure communication. In *Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL'01, pages 104–115, New York, NY, USA, 2001. ACM.

[3] Franz Baader and Tobias Nipkow. *Term rewriting and all that.* Cambridge University Press, New York, NY, USA, 1998.

[4] Ştefan Ciobâcă, Stéphanie Delaune, and Steve Kremer. Computing knowledge in security protocols under convergent equational theories. *J. Autom. Reasoning*, 48(2):219–262, 2012.

[5] R. Diestel. *Graph Theory.* Springer, third edition.

[6] P. Narendran, F. Pfenning, and R. Statman. On the unification problem for cartesian closed categories. In *Proceedings, Eighth Annual IEEE Symposium on Logic in Computer Science*, pages 57–63. IEEE Computer Society Press, 1993.