Symbolic Protocol Analysis for Monoidal Equational Theories (How Algebra Helps to Solve Intruder Constraints)

Ralf Treinen
joint work with
Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez

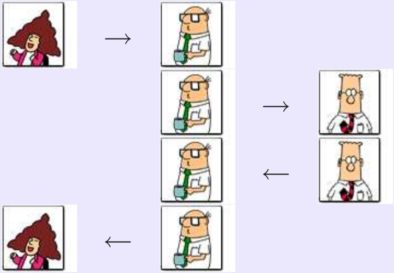
LSV, CNRS UMR 8643, ENS de Cachan & INRIA Futurs
LIF, Université Aix-Marseille 1 & CNRS UMR 6166

February 14, 2007

TMN Protocol: Distribution of a fresh session key

[Tatebayashi, Matsuzuki, Newmann 89]:

A $\quad W \quad$ D



$A \rightarrow W$: $A, D, \{N_A\}_{Pub_W}$

$W \rightarrow D$: W, A

$D \rightarrow W$: $D, A, \{N_D\}_{Pub_W}$

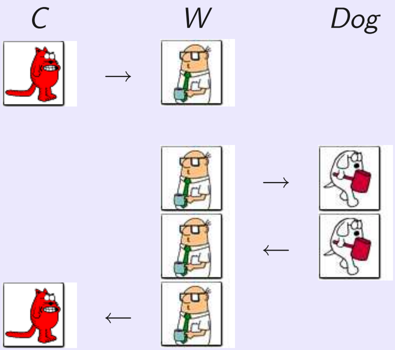
$W \rightarrow A$: $W, D, N_A \oplus N_D$

Alice retrieves N_D:

Using $x \oplus x \oplus y = y$, knowing N_A and N_D, she deduces N_D.

Attack on TMN Protocol

With homomorphic encryption



$C \rightarrow W$: $C, Dog, \underbrace{\{N_A\}_{Pub_W} * \{N_C\}_{Pub_W}}_{\{N_A * N_C\}_{Pub_W}}$

$W \rightarrow Dog$: W, C

$W \leftarrow Dog$: $Dog, C, \{N_{Dog}\}_{Pub_W}$

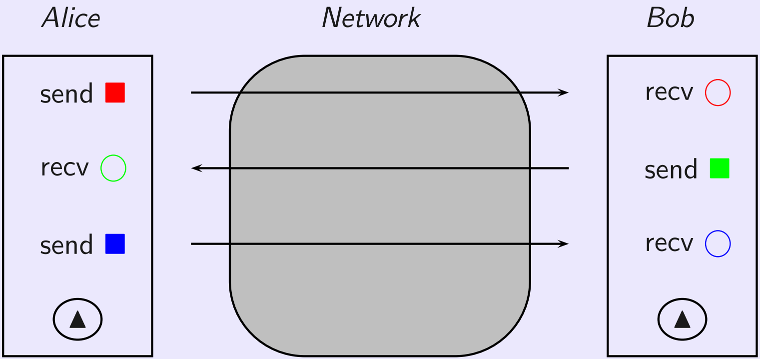
$C \leftarrow W$: $W, N_A * N_C \oplus N_{Dog}$

Catbert Learns:

Using $x \oplus x \oplus y = y$, knowing N_C and N_{Dog}, he deduces N_A.

Intended Execution of Protocols

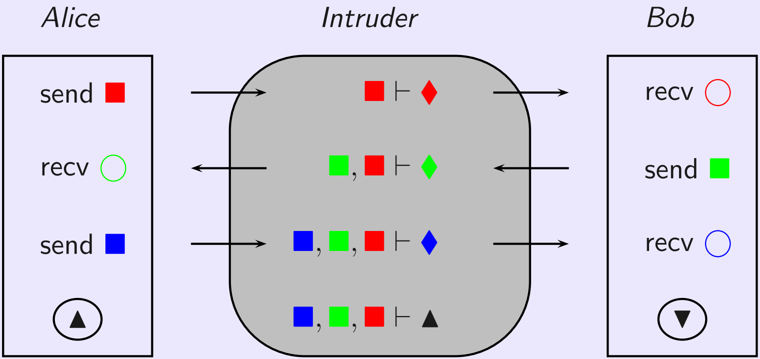
Execution of a Protocol between 2 Agents



■, ▲: message , ◯: pattern.

The Intruder is the Network

Intruder can deduce messages by $\vdash$



■, ▲, ♦ : message ; ○: pattern ; $\vdash$: intruder deduction

Constraint System for *Symbolic Trace Reachability*

- choose number of instances of the protocol
- guess a linearisation of the execution

$$
\begin{array}{lcl}
t_0, \ldots, t_n & \Vdash & u_1 \\
\vdots & \vdots & \vdots \\
t_0, \ldots, t_n, \ldots, t_k & \Vdash & u_{k+1} = \mathit{secret}
\end{array}
$$

Satisfiability is NP-complete [Rusinowitch, Turuani '03].

Symbolic trace reachability is undecidable if number of sessions not bounded.

Example: TMN protocol

Protocol

$$\begin{array}{lllll} 1. & A & \rightarrow & S: & A, B, h(K_a) \\ 2. & S & \rightarrow & B: & S, A \\ 3. & B & \rightarrow & S: & B, A, h(K_b) \\ 4. & S & \rightarrow & A: & S, B, K_b + K_a \end{array}$$

Constraint system for one session, simplified

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$

$$\mathcal{C} \quad := \quad \begin{cases} T_0 \Vdash X_a, X_b, h(Y_a) & S \text{ receives a request from } I \\ T_1 := T_0, S, X_a & S \text{ answers the request to } X_b \\ T_1 \Vdash X_b, X_a, h(Y_b) & S \text{ receives the answer of } X_b \\ T_2 := T_1, S, X_b, Y_a + Y_b & S \text{ answers the request to } I \\ T_2 \Vdash K_b & \text{the secret } K_b \text{ is revealed} \end{cases}$$

If this system has a solution then the secret K_b can be obtain by the Intruder.

Perfect Cryptography Assumption

Knowledge about some encrypted message can only be obtained when the encryption key is known.

Weakening of the Perfect Cryptography Assumption

Cryptographic primitives have properties which

- are necessary for the protocol
- can be exploited by an intruder

Algebraic properties: expressed by equational axioms

Our contribution

Generic approach for the class of *monoidal equational theories*.

Outline

Outline

Unification

Given an equational theory E.
A substitution μ is a *unifier* of two terms s and t if

$$s\mu =_E t\mu$$

Unification

Given an equational theory E.
A substitution μ is a *unifier* of two terms s and t if

$$s\mu =_E t\mu$$

Most General Unifier

A set C of substitutions is *most general set of unifiers* of terms s, t if

- Every $\mu \in C$ is a unifier of s, t
- Every unifier of s and t is an instance of some $\mu \in C$.

Note: A minimal most general set of unifiers may be singleton, non-singleton, infinite, or even not exist (depends on E, and on the presence of free constant and function symbols in s, t).

Why is unification important when solving intruder constraints?

- Unification is used in the resolution procedure (as we will see later).
- [Delaune'06] : Decidability of unification is necessary for decidability of intruder constraints.

Definition [Baader, Nutt]

An equational theory E is *monoidal* if

- The signature consists of 0, $+$, possibly some unitary symbols;
- $+$ is associative and commutative, with unit 0;
- all unitary functions are *endomorphisms*.

Definition [Baader, Nutt]

An equational theory E is *monoidal* if

- The signature consists of 0, $+$, possibly some unitary symbols;
- $+$ is associative and commutative, with unit 0;
- all unitary functions are *endomorphisms*.

Examples of monoidal theories

- ACU: simplest example
  - Associativity (A) : $x + (y + z) = (x + y) + z$
  - Commutativity (C) : $x + y = y + x$
  - Unit (U) : $x + 0 = x$

More examples of monoidal theories

- ACUI
  - Axioms ACU
  - Idempotency (I) : $x + x = x$
- ACUN : theory of *exclusive or*
  - Axioms ACU
  - Nilpotency (N) : $x + x = 0$
- AG : Abelian Groups
  - Unitary function $-$
  - Axioms ACU
  - Homomorphism : $-(x + y) = (-x) + (-y)$
  - Inverse : $x + (-x) = 0$

Examples of monoidal theories with (more) endomorphisms

- ACUh
  - Axioms ACU
  - Homomorphism (h) : $h(x+y) = h(x) + h(y)$, $h(0) = 0$.
- ACUIh, ACUNh, AGh : analogous
- Add several homomorphisms.
- Add several *commuting* homomorphisms
  - h and g commute : $h(g(x)) = g(h(x))$

Semiring $\mathcal{S}_{\mathsf{E}}$ associated to monoidal theory E [Nutt'90]

- Universe: terms over signature of E and one variable $\mathbf{1}$, modulo E.
- Definition of 0, $+$ in $\mathcal{S}_{\mathsf{E}}$: as in terms modulo E.
- Definition of multiplication $\cdot$ in $\mathcal{S}_{\mathsf{E}}$:

$$s \cdot t = s[\mathbf{1} \mapsto t]$$

Semiring $\mathcal{S}_\mathsf{E}$ associated to monoidal theory E [Nutt'90]

- Universe: terms over signature of E and one variable $\mathbf{1}$, modulo E.
- Definition of 0, $+$ in $\mathcal{S}_\mathsf{E}$: as in terms modulo E.
- Definition of multiplication $\cdot$ in $\mathcal{S}_\mathsf{E}$:

$$s \cdot t = s[\mathbf{1} \mapsto t]$$

Consequence: $\mathbf{1}$ is the multiplicative unit

- $\mathbf{1} \cdot t = \mathbf{1}[\mathbf{1} \mapsto t] = t$
- $t \cdot \mathbf{1} = t[\mathbf{1} \mapsto \mathbf{1}] = t$

Example: The semiring for ACUN

- Universe: $\{0, 1\}$
- $0 + 0 = 0 = 1 + 1$, $0 + 1 = 1 = 1 + 0$
- $0 \cdot 0 = 0 = 0 \cdot 1 = 1 \cdot 0$, $1 \cdot 1 = 1$
- Semiring is isomorphic to the finite field $\mathcal{Z}/2\mathcal{Z}$.

Example: The semiring for ACUN

- Universe: $\{0, 1\}$
- $0 + 0 = 0 = 1 + 1$, $0 + 1 = 1 = 1 + 0$
- $0 \cdot 0 = 0 = 0 \cdot 1 = 1 \cdot 0$, $1 \cdot 1 = 1$
- Semiring is isomorphic to the finite field $\mathcal{Z}/2\mathcal{Z}$.

Example: The semiring for AGh

- Universe: $\mathcal{Z}[\mathrm{h}]$
- Addition and multiplication as usual over polynomials
- Semiring is isomorphic to the commutative ring $\mathcal{Z}[\mathrm{h}]$.

More properties of $\mathcal{S}_\mathsf{E}$ [Nutt '90]

- $\mathcal{S}_\mathsf{E}$ is a ring iff E is a *group theory* :

$$x + t =_E 0 \text{ for some } t$$

- $\mathcal{S}_\mathsf{E}$ is commutative iff the homomorphisms in E commute :

$$h_1(h_2(x)) =_E h_2(h_1(x)) \text{ for any unitary } h_1,\ h_2$$

Unification in monoidal theories [Baader, Nutt]

Let E be a monoidal equational theory such that

- Unification without additional symbols is finitary (i.e., any solvable unification problem has a finite complete set of unifiers)
- There is an algorithm that finds a solution to any inhomogeneous linear system of equations, and a basis of the solutions of any homogeneous system of linear equations over $\mathcal{S}_{\mathsf{E}}$

Then there is an algorithm that computes a finite complete set of unifiers for any unification problem with free function symbols.

(Positive) Results for some Monoidal Theories

- ACUN (exclusive or) : decidable in NP
  [Rusinowitch & al 03] [Comon-Shmatikov 03]
- AG (Abelian Group) : decidable in NP
  [Millen-Shmatikov 05]
- ACUNh (exclusive or with homomorphism) : decidable
  [DLLT 06]

Outline

Inference System: Dolev-Yao with rewriting

(A) $\dfrac{u \in T}{T \vdash u}$ (UL) $\dfrac{T \vdash \langle u, v\rangle}{T \vdash u}$

(P) $\dfrac{T \vdash u \qquad T \vdash v}{T \vdash \langle u, v\rangle}$ (UR) $\dfrac{T \vdash \langle u, v\rangle}{T \vdash v}$

(C) $\dfrac{T \vdash u \qquad T \vdash v}{T \vdash \{u\}_v}$ (D) $\dfrac{T \vdash \{u\}_v \qquad T \vdash v}{T \vdash u}$

(M_E) $\dfrac{T \vdash u_1 \quad \cdots \quad T \vdash u_n}{T \vdash C[u_1, \ldots, u_n]\downarrow}$ C is an context made with $\{h, +\}$

Example for M_E

$$\frac{T \vdash a + h(a) \quad T \vdash b}{T \vdash a + h^2(a) + h(b)} \qquad C[u_1, u_2] = u_1 + h(u_1) + h(u_2)$$

Relation $\vdash$

Deduction relation as defined by the inference system.

Relation $\vdash$

Deduction relation as defined by the inference system.

Relation $\vdash_{\mathsf{M_E}}$

$t_1, \ldots, t_n \vdash_{\mathsf{M_E}} t$ if deduction in exactly one step using rule M_E

Relation $\vdash$

Deduction relation as defined by the inference system.

Relation $\vdash_{\mathsf{M_E}}$

$t_1, \ldots, t_n \vdash_{\mathsf{M_E}} t$ if deduction in exactly one step using rule M_E

Lemma

If solvability of inhomogeneous systems of linear equations over $\mathcal{S}_{\mathsf{E}}$ is decidable then $\vdash_{\mathsf{M_E}}$ is decidable.

Subterms (Example)

$$St_{\mathsf{E}}(h^2(a) + b + c) = \{h^2(a) + b + c, a, b, c\}.$$

Subterms (Example)

$St_{\mathsf{E}}(h^2(a) + b + c) = \{h^2(a) + b + c, a, b, c\}.$

Theorem of Locality [LLT'05,Del'05]

A minimal proof P of $T \vdash u$ contains only terms in $St_{\mathsf{E}}(T \cup \{u\})$.

Subterms (Example)

$St_{\mathsf{E}}(h^2(a) + b + c) = \{h^2(a) + b + c, a, b, c\}$.

Theorem of Locality [LLT'05,Del'05]

A minimal proof P of $T \vdash u$ contains only terms in $St_{\mathsf{E}}(T \cup \{u\})$.

Decidability of Intruder Deduction

$T \vdash u$ (for T, u ground) is decidable if solvability of inhomogeneous systems of equations over Se_{E} is decidable.

The proof is based on McAllester's locality theorem, and on the lemma on deciding $\vdash_{\mathsf{M_E}}$.

Outline

Deterministic Protocol

Definition

$$P \quad := \quad \begin{cases} u_1 \longrightarrow v_1 \\ u_2 \longrightarrow v_2 \\ \vdots \\ u_n \longrightarrow v_n \end{cases}$$

A protocol P is deterministic iff:
for all ground substitutions τ, σ and for all $i \in [1, \ldots n]$:
if $u_1\tau =_E u_1\sigma, \ldots, u_i\tau =_E u_i\sigma$ then $v_i\tau =_E v_i\sigma$.

Determinism is decidable if there is an algorithm to compute finite complete sets of unifiers.

Reminder: Constraint System

$$\mathcal{C} \quad := \quad \begin{cases} T_1 & \Vdash & u_1 \\ T_2 & \Vdash & u_2 \\ \vdots & \vdots & \vdots \\ T_k & \Vdash & u_k \end{cases}$$

where

- $T_1 \subseteq T(F)$
- $T_2, \ldots, T_k \subseteq T(F, X)$
- $u_1, \ldots, u_k \in T(F, X)$

System of Constraints Well-formed [Millen-Shmatikov 03]

$\mathcal{C} = \{T_i \Vdash u_i\}_{1 \leq i \leq k}$ is *well-formed* if:

- *monotonicity*: The knowledge of the intruder is increasing.

$$T_1 \subseteq T_2 \subseteq \ldots \subseteq T_k$$

- *origination*: Variables appear first on right side:

$$x \in vars(T_i) \Rightarrow \exists j < i : x \in vars(u_j)$$

System of Constraints Well-formed [Millen-Shmatikov 03]

$\mathcal{C} = \{T_i \Vdash u_i\}_{1 \leq i \leq k}$ is *well-formed* if:

- *monotonicity*: The knowledge of the intruder is increasing.

$$T_1 \subseteq T_2 \subseteq \ldots \subseteq T_k$$

- *origination*: Variables appear first on right side:

$$x \in vars(T_i) \Rightarrow \exists j < i : x \in vars(u_i)$$

System of Constraints Well-defined [Millen-Shmatikov 03]

$\mathcal{C}$ is *well-defined* if for every substitution θ, $\mathcal{C}\theta$ is well-formed.

Well-definedness: Example 1

The Constraint System from the TMN Example is Well-Defined

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$
Equational theory: ACUNh

$$\mathcal{C} \quad := \quad \begin{cases} T_0 & \Vdash \quad X_a, X_b, h(Y_a) \\ T_0, S, X_a & \Vdash \quad X_b, X_a, h(Y_b) \\ T_0, S, X_a, S, X_b, Y_a + Y_b & \Vdash \quad K_b \end{cases}$$

Well-Definedness: Example 2, $E = ACUN$

The Constraint System

$$\mathcal{C} \quad := \quad \begin{cases} T_0 & \Vdash \quad X + Y \\ T_0, X & \Vdash \quad c \end{cases}$$

Well-Definedness: Example 2, $E = ACUN$

The Constraint System

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lcl} T_0 & \Vdash & X + Y \\ T_0, X & \Vdash & c \end{array} \right.$$

Monotonicity OK !

Well-Definedness: Example 2, $E = ACUN$

The Constraint System

$$\mathcal{C} \quad := \quad \begin{cases} T_0 & \Vdash \quad X + Y \\ T_0, X & \Vdash \quad c \end{cases}$$

Monotonicity OK !

Origination OK !

Well-Definedness: Example 2, $E = ACUN$

The Constraint System

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lcl} T_0 & \Vdash & X + Y \\ T_0, X & \Vdash & c \end{array} \right.$$

Monotonicity OK !

Origination OK !

But NOT well-defined !

$\theta = \{Y \to X\}$ and $\mathcal{C}\theta$ is not well-formed:

$$\mathcal{C}\theta \quad := \quad \left\{ \begin{array}{lcl} T_0 & \Vdash & 0 \\ T_0, X & \Vdash & c \end{array} \right.$$

Lemma

Deterministic protocol $\Rightarrow$ well-defined constraint system.

Example: Non well-defined constraint system:

$$\mathcal{C} \quad := \quad \begin{cases} T_0 & \Vdash \quad X + Y \\ T_0, X & \Vdash \quad c \end{cases}$$

Witness of non-welldefinedness: $\theta = \{Y \rightarrow X\}$
Corresponding protocol: $P : X + Y \rightarrow X$
is non-deterministic:
On reception of message 0, one can

- send out a since $a + a = 0$
- send out b since $b + b = 0$

Outline

Conservative Solution

Conservative solution σ

σ does not introduce structure not already in $\mathcal{C}$.

Example:

$$\begin{array}{lcl} 0, a, h(b) & \Vdash & h(x) \\ 0, a, h(b), x & \Vdash & \langle a, b \rangle \end{array}$$

$\sigma = \{x \mapsto \langle a, a \rangle + b\}$ is a non-conservative solution.
since $\langle a, a \rangle$ is not a structure of $\mathcal{C}$.

However, $\rho = \{x \mapsto b\}$ is a conservative solution of $\mathcal{C}$.

Conservative Solution

Conservative solution σ

σ does not introduce structure not already in $\mathcal{C}$.

Example:

$$\begin{array}{lcl} 0, a, h(b) & \Vdash & h(x) \\ 0, a, h(b), x & \Vdash & \langle a, b \rangle \end{array}$$

$\sigma = \{x \mapsto \langle a, a \rangle + b\}$ is a non-conservative solution.
since $\langle a, a \rangle$ is not a structure of $\mathcal{C}$.

However, $\rho = \{x \mapsto b\}$ is a conservative solution of $\mathcal{C}$.

Lemma

Let $\mathcal{C}$ be a well-defined constraint system. If there exists a solution σ of $\mathcal{C}$ then there exists a conservative one.

Lifting Locality Lemma

Lifting Locality Lemma

Let σ be a conservative solution of $\mathcal{C} = \{C_1, \ldots, C_k\}$.
For each $i \leq k$, there exists a proof P_i of $C_i\sigma$ that involves only terms in $St_{\mathsf{E}}(\mathcal{C})\sigma$.

Outline

From Constraints to One-step Constraints

Non-deterministic step:

- Guess the subterms used in the steps of the deduction.
- Guess the order in which they are deduced.
- Construct the corresponding *one-step deduction* constraint system.

Justified by the lemma on conservative solutions.

Example

TMN Example

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$
$T_1 := T_0, S, X_a$
$T_2 := T_1, S, X_b, Y_a + Y_b$

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lcl} T_0 & \Vdash & X_a, X_b, h(Y_a) \\ T_1 & \Vdash & X_b, X_a, h(Y_b) \\ T_2 & \Vdash & K_b \end{array} \right.$$

We obtain a well-defined constraint system.

Example

TMN Example

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$
$T_1 := T_0, S, X_a$
$T_2 := T_1, S, X_b, Y_a + Y_b$

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lll} T_0 & \Vdash & X_a, X_b, h(Y_a) \\ T_1 & \Vdash & X_b, X_a, h(Y_b) \\ T_2 & \Vdash & K_b \end{array} \right.$$

We obtain a well-defined constraint system.

Guess set of subterms of $\mathcal{C}$ and an order on these subterms

$S_0 = \{X_a, X_b, h(Y_a)\}$ $S_1 = \{Y_b, h(Y_b)\}$ and $S_2 = \{K_b\}$.

$$\mathcal{C}' \quad := \quad \left\{ \begin{array}{lll} T_0 & \Vdash_1 & X_a \\ T_0, X_a & \Vdash_1 & X_b \\ T_0, X_a, X_b & \Vdash_1 & h(Y_a) \\ T_0, X_a, X_b, h(Y_a) & \Vdash_1 & X_a, X_b, h(Y_a) \\ T_1, S_0 & \Vdash_1 & Y_b \\ T_1, S_0, Y_b & \Vdash_1 & h(Y_b) \\ T_1, S_0, Y_b, h(Y_b) & \Vdash_1 & X_b, X_a, h(Y_b) \\ T_2, S_0, S_1 & \Vdash_1 & K_b \end{array} \right.$$

From One-step Constraints to M_E Constraints

Non-deterministic step:

- Guess equalities between subterms of $\mathcal{C}$ (uses a unification property: there is a finite most general set of unifiers)
- Consider all the possible applications of rules (C) (P) (D) (UR) (UL)
- Check that all one-step deduction constraints, except for $\Vdash_{\mathsf{M_E}}$, are satisfied.

Example

Example

$$\mathcal{C} \quad := \quad \begin{cases} \langle a, b\rangle & \Vdash_1 \quad \langle X, b\rangle \\ \langle a, b\rangle, X + b & \Vdash_1 \quad Y + \langle a, b\rangle a \end{cases}$$

Guess $\{\langle X, b\rangle = \langle a, b\rangle\}$, compute ACUNh m.g.u. $\theta : \{X \mapsto a\}$

$$\mathcal{C}\theta \quad := \quad \begin{cases} \langle a, b\rangle & \Vdash_{M_E} \quad \langle a, b\rangle \\ \langle a, b\rangle, a + b & \Vdash_{M_E} \quad Y + \langle a, b\rangle \end{cases}$$

Protocol is still well-defined, has a non-collapsing solution.

TMN Example

Substitution

We guess on $St_E(\mathcal{C}')$,
$R = \{X_a = I; X_b = C; Y_b = K_i; K_b = Y_a + Y_b\}$.
Compute ACUNh m.g.u. from R:
$\theta = \{X_a \mapsto I; X_b \mapsto C; Y_b \mapsto K_i; Y_a \mapsto K_b + K_i\}$.

$\mathcal{C}\theta$ is ground, every constraint is satisfied then there is an ATTACK.

Retrieve the real ATTACK

TMN Protocol

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{ll} T_0 \Vdash X_a, X_b, h(Y_a) & \text{S receives a request from I} \\ T_1 := T_0, S, X_a & \text{S answers the request to X_b} \\ T_1 \Vdash X_b, X_a, h(Y_b) & \text{S receives the answer of X_b} \\ T_2 := T_1, S, X_b, Y_a + Y_b & \text{S answers the request to I} \\ T_2 \Vdash K_b & \text{the secret K_b is revealed} \end{array} \right.$$

$\theta = \{X_a \mapsto I; X_b \mapsto C; Y_b \mapsto K_i; Y_a \mapsto K_b + K_i\}$

$$\mathcal{C}\theta \quad := \quad \left\{ \begin{array}{ll} T_0 \Vdash I, C, h(K_b + K_i) & \text{S receives a request from I} \\ T_1 := T_0, S, I & \text{S answers the request to C} \\ T_1 \Vdash C, I, h(K_i) & \text{S receives the answer of C} \\ T_2 := T_1, S, C, K_b + K_i + K_i & \text{S answers the request to I} \\ T_2 \Vdash K_b & \text{the secret K_b is revealed} \end{array} \right.$$

Abstraction of Factors (I)

Idea

Abstraction ρ replaces all factors by new constant symbols to get a constraint system on signature:$+$, h, and constant symbols.

Example:

$$\mathcal{C} \quad := \quad \begin{cases} a, b & \Vdash_{M_E} \quad \langle X, b \rangle \\ a, b, X & \Vdash_{M_E} \quad X + b \end{cases}$$

$\mathcal{C}$ is well-defined, but not $\mathcal{C}\rho$

$$\mathcal{C}\rho \quad := \quad \begin{cases} a, b & \Vdash_{M_E} \quad c_1 \\ a, b, X & \Vdash_{M_E} \quad X + b \end{cases}$$

Abstraction of Factors (II)

$\mathcal{C}$ is Factor-Preserving

Every non-variable factor appearing on the on right side of a constraint also appears on the left side of the same constraint.

Lemma

- Well-defined + non-collapsing solution $\Rightarrow$ Factor-Preserving.
- If $\mathcal{C}$ is W.D. and Factor-Preserving then $\mathcal{C}\rho$ is W.D.

Example:

$$\mathcal{C} \quad := \quad \begin{cases} a, b & \Vdash_{M_E} \quad X + Y \\ a, b, \langle X + Y, b \rangle & \Vdash_{M_E} \quad \langle X + Y, b \rangle + Z \end{cases}$$

$$\mathcal{C}\rho \quad := \quad \begin{cases} a, b & \Vdash_{M_E} \quad X + Y \\ a, b, c_1 & \Vdash_{M_E} \quad c_1 + Z \end{cases}$$

The case of a finite semiring $\mathcal{S}_{\mathsf{E}}$

Theorem 1

Let E be a monoidal equational theory represented by an AC-convergent rewrite system, disjoint from the standard operators.
If the associated semiring $\mathcal{S}_{\mathsf{E}}$ is finite, then satisfiability of well-defined constraint systems is decidable.

The case of a finite semiring $\mathcal{S}_\mathsf{E}$

Theorem 1

Let E be a monoidal equational theory represented by an AC-convergent rewrite system, disjoint from the standard operators.
If the associated semiring $\mathcal{S}_\mathsf{E}$ is finite, then satisfiability of well-defined constraint systems is decidable.

Application

The theory $ACUN$ (theory of exclusive or):
The associated semiring is $\mathcal{Z}/2\mathcal{Z}$.

New Characterization of well-defined over $\{+, h\}$

Example:

$$\begin{array}{lll} a, b & \Vdash_{\mathsf{M_E}} & u_1 = X_1 + X_2 + a \\ a, b, h(X_1) + h(X_2) & \Vdash_{\mathsf{M_E}} & u_2 = h(X_1) + h(b) \\ a, b, h(X_1) + h(X_2), h(X_2) & \Vdash_{\mathsf{M_E}} & u_3 = a + b \end{array}$$

We obtain

$$\begin{array}{lll} \vec{u_1} & = & (1, 1) \\ \vec{u_2} & = & (h, 0) \\ \vec{u_3} & = & (0, 0) \end{array}$$

Basis $\mathcal{B} = \{\vec{u_1}, \vec{u_2}\}$

New Characterization of well-defined over $\{+, h\}$

Example:

$$\begin{array}{lll} a, b & \Vdash_{\mathsf{M_E}} & u_1 = X_1 + X_2 + a \\ a, b, h(X_1) + h(X_2) & \Vdash_{\mathsf{M_E}} & u_2 = h(X_1) + h(b) \\ a, b, h(X_1) + h(X_2), h(X_2) & \Vdash_{\mathsf{M_E}} & u_3 = a + b \end{array}$$

We obtain

$$\begin{array}{rcl} \vec{u_1} & = & (1,1) \\ \vec{u_2} & = & (h,0) \\ \vec{u_3} & = & (0,0) \end{array}$$

Basis $\mathcal{B} = \{\vec{u_1}, \vec{u_2}\}$

Characterization

Let $\mathcal{C} = \{t_1, \ldots, t_{n+i-1} \Vdash_{\mathsf{M_E}} u_i\}_{i=1,\ldots,k}$ on signature $\{+, h\}$.
C is W.D. iff $\forall i \leq k, \{\vec{t}_{n+i-1}\} \cup \{\vec{u_j} \in \mathcal{B} \mid j < i\}$ are dependent.

New Characterization of well-defined over $\{+, h\}$

Example:

$$\begin{array}{lll} a, b & \Vdash_{\mathsf{M_E}} & X_1 + X_2 + a \\ a, b, h(X_1) + h(X_2) & \Vdash_{\mathsf{M_E}} & h(X_1) + h(b) \\ a, b, h(X_1) + h(X_2), h(X_2) & \Vdash_{\mathsf{M_E}} & a + b \end{array}$$

$\vec{u_1} = (1, 1),\ \vec{u_2} = (h, 0),\ B = \{\vec{u_1}, \vec{u_2}\}$

Characterization

Let $\mathcal{C} = \{t_1, \ldots, t_{n+i-1} \Vdash_{\mathsf{M_E}} u_i\}_{i=1,\ldots,k}$ on signature $\{+, h\}$.
C is W.D. iff $\forall i \leq k, \{\vec{t}_{n+i-1}\} \cup \{\vec{u_j} \in \mathcal{B} \mid j < i\}$ are dependent.

On the example:

$\{(h, h)\} \cup \{(1, 1)\}$ and $\{(0, h)\} \cup \{(1, 1), (h, 0)\}$ are dependent.

From M_E Constraints to Quadratic Equation Systems

Constraints M_E

$$
\begin{array}{lll}
h(a)+a, b+h^2(a) & \Vdash_{\mathrm{M_E}} & h(X_1)+h^2(X_2) \\
h(a)+a, b+h^2(a), X_1+h(X_2) & \Vdash_{\mathrm{M_E}} & X_1+a \\
h(a)+a, b+h^2(a), X_1+h(X_2), h(X_1)+h(a) & \Vdash_{\mathrm{M_E}} & h(X_1)+h^2(X_2)+X_1+a
\end{array}
$$

NOTATION: $t_1 = h(a)+a$ and $t_2 = b+h^2(a)$.

System of equations

$$
\begin{array}{lll}
z[1,1]t_1 + z[1,2]t_2 & = & h(X_1)+h^2(X_2) \\
z[2,1]t_1 + z[2,2]t_2 + z[2,3](X_1+h(X_2)) & = & X_1+a \\
z[3,1]t_1 + z[3,2]t_2 + z[3,3](X_1+h((X_2))+z[3,4](h(X_1)+h(a)) & = & \\
 & & h(X_1)+h^2(X_2)+X_1+a
\end{array}
$$

Solvability of a quadratic system of equations is in general undecidable.

Euclidean rings

Definition

An *Euclidean ring* is a commutative ring R

- without zero divisors
- with division algorithm: there is a norm $v : R - \{0\} \rightarrow \mathcal{N}$ with:

$$\forall a, b \in R, b \neq 0 \exists q, r \in S : a = bq + r, (r = 0 \text{ or } v(r) < v(b))$$

Examples of Euclidean Rings

- The ring $\mathcal{Z}$
- The ring of polynomials $\mathbf{K}[h]$ for any field $\mathbf{K}$.

Solving Well-defined Quadratic Systems

Bound the Contexts of Well-defined Systems

If there exists a solution then there exists a solution where $z[i,j]$ are bounded by $Q_{max} = det(\vec{u_1}, \ldots, \vec{u_n})$ for Basis $\{\vec{u_1}, \ldots, \vec{u_n}\}$.

Example

$Q_{max} = det(\vec{u}_1, \vec{u}_2) = det \begin{pmatrix} h & h^2 \\ 1 & 0 \end{pmatrix} = h^2$.

$$\begin{array}{l} z[1,1]t_1 + z[1,2]t_2 = h(X_1) + h^2(X_2) \\ z[2,1]t_1 + z[2,2]t_2 + z[2,3](X_1 + h(X_2)) = X_1 + a \end{array}$$

$\rho_1 = \{z[1,1] \mapsto 0; z[1,2] \mapsto h; z[2,1] \mapsto h+1; z[2,2] \mapsto 1; z[2,3] \mapsto 0\}$.

$$\begin{array}{l} h \odot (b + h^2(a)) = h(X_1) + h^2(X_2) \\ (h+1) \odot (h(a) + a) + 1 \odot (b + h^2(a)) = X_1 + a \end{array}$$

$\theta = \{X_1 \mapsto b, X_2 \mapsto h(a)\}$.
Verify that θ satisfies the others constraints.

The case of an Euclidean semiring $\mathcal{S}_{\mathsf{E}}$

Theorem 2

Let E be a monoidal equational theory represented by an AC-convergent rewrite system, disjoint from the standard operators.
If

- the associated semiring $\mathcal{S}_{\mathsf{E}}$ is Euclidean, and $\{x \mid v(x) < v(q)\}$ is finite for any $q \in \mathcal{S}_{\mathsf{E}}$
- elementary unification is unary, and there exists an algorithm to solve inhomogeneous systems of linear equations

then satisfiability of well-defined constraint systems is decidable.

Applications

- The theory *ACUNh* (theory of exclusive or with homomorphism):
  The associated semiring is $\mathcal{Z}/2\mathcal{Z}[h]$.
- The theory *AG* (theory of Abelian Groups):
  The associated semiring is $\mathcal{Z}$.

Outline

Our Procedure

Given: Deterministic protocol.

1. Guess order of execution $\Rightarrow$ constraint system (well-defined)
2. Guess partition of subterms $\Rightarrow$ one-step constraint system (well-defined)
3. Guess equality between subterms $\Rightarrow$ M_E constraint system (well-defined and factor-preserving)
4. Abstraction $\Rightarrow$ System of equations on $\mathcal{S}_{\mathsf{E}}$ (well-defined)
5. Solve system of equations $\Rightarrow$ Attack if solution

Overview

Theory E	$\mathcal{S}_E$	Properties of $\mathcal{S}e_E$	E. Unificat.	Constraints
ACU	$\mathbb{N}$	semiring	unitary	?
ACUI	$\mathbb{B}$	finite semiring	unitary	decidable
ACUN	$\mathbb{Z}/2\mathbb{Z}$	finite semiring	unitary	decidable
AG	$\mathbb{Z}$	Euclidean ring	unitary	decidable
ACUh	$\mathbb{N}[\mathrm{h}]$	semiring	undecidable	undecidable
ACUIh	$\mathbb{B}[\mathrm{h}]$	semiring	type 0	?
ACUNh	$\mathbb{Z}/2\mathbb{Z}[h]$	Euclidean ring	unitary	decidable
AGh	$\mathbb{Z}[\mathrm{h}]$	commutative ring	unitary	undecidable

Example: TMN protocol

Protocol

$$\begin{array}{llcll}
1. & A & \rightarrow & S: & A, B, h(K_a) \\
2. & S & \rightarrow & B: & S, A \\
3. & B & \rightarrow & S: & B, A, h(K_b) \\
4. & S & \rightarrow & A: & S, B, K_b + K_a
\end{array}$$

Constraint system (for one session)

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{ll}
T_0 \Vdash X_a, X_b, h(Y_a) & S \text{ receives a request from } I \\
T_1 := T_0, S, X_a & S \text{ answers the request to } X_b \\
T_1 \Vdash X_b, X_a, h(Y_b) & S \text{ receives the answer of } X_b \\
T_2 := T_1, S, X_b, Y_a + Y_b & S \text{ answers the request to } I \\
T_2 \Vdash K_b & \text{the secret } K_b \text{ is revealed}
\end{array} \right.$$

If this system has a solution then the secret K_b can be obtain by the Intruder.

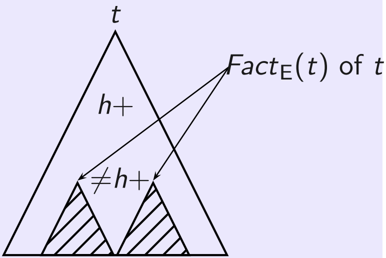
Standard Terms and Factors

t is *standard* if $t \neq f(u)$ where $f \in \{+, h\}$

$Fact_{\mathsf{E}}(t)$: top-level standard subterms of t

Example:
$t_1 = h^2(a) + b + c$
$Fact_{\mathsf{E}}(t_1) = \{a, b, c\}$

$t_2 = h(\langle a, b\rangle) + c$
$Fact_{\mathsf{E}}(t_2) = \{\langle a, b\rangle, c\}$



Subterms

The set of *subterms* :

- if $t = f(t_1, \ldots, t_n)$ standard:
  $St_{\mathsf{E}}(t) = \{t\} \cup St_{\mathsf{E}}(t_1) \cup \ldots \cup St_{\mathsf{E}}(t_n)$
- if $t = f(t_1, \ldots, t_n)$ non-standard:
  $St_{\mathsf{E}}(t) = \{t\} \cup St_{\mathsf{E}}(Fact_{\mathsf{E}}(t_1)) \cup \ldots \cup St_{\mathsf{E}}(Fact_{\mathsf{E}}(t_n))$

Example:

$t_1 = h^2(a) + b + c$
$St_{\mathsf{E}}(t_1) = \{t_1, a, b, c\}.$

$t_2 = h(\langle a, b\rangle) + c$
$St_{\mathsf{E}}(t_2) = \{t_2, \langle a, b\rangle, a, b, c\}.$