An Algebra for Symbolic Diffie-Hellman Protocol Analysis

Daniel J. Dougherty and Joshua D. Guttman
Worcester Polytechnic Institute
The MITRE Corporation

March 2013
Bertinoro International Spring School

Thanks to the US National Science Foundation, under grant 1116557

guttman@wpi.edu

Ephemeral DH

the optimistic view

$$
\begin{tikzcd}
A & \bullet \arrow[r, Rightarrow] \arrow[d, "g^x"] & \bullet \arrow[r, Rightarrow] & K_A \doteq (g^y)^x \\
B & \bullet \arrow[r, Rightarrow] & \bullet \arrow[r, Rightarrow] \arrow[u, "g^y"'] & K_B \doteq (g^x)^y
\end{tikzcd}
$$

$$K_A = (g^y)^x \;=\; (g^x)^y = K_B$$

in a cyclic group of prime order q

Amazing outcome: Shared secret via public information

Ephemeral DH

the realistic view

$$
\begin{tikzcd}
A & \bullet \arrow[r, Rightarrow] \arrow[d, "g^x"] & \bullet \arrow[r, Rightarrow] & K_A \doteq (R_B)^x \\
 & {} & {} \arrow[u, "R_B"'] & \\
 & {} \arrow[d, "R_A"] & {} & \\
B & \bullet \arrow[r, Rightarrow] & \bullet \arrow[r, Rightarrow] \arrow[u, "g^y"'] & K_B \doteq (R_A)^y
\end{tikzcd}
$$

If $R_A = g^x$ and $R_B = g^y$

then shared secret established

Ephemeral DH

the realistic view

$$
\begin{tikzcd}
A & \bullet \arrow[r, Rightarrow] \arrow[d, "g^x"] & \bullet \arrow[r, Rightarrow] & K_A \doteq (R_B)^x \\
 & {} & {} \arrow[u, "R_B"'] & \color{red}{K_A \ \bullet} \\
 & {} \arrow[d, "R_A"] & {} & \color{red}{K_B \ \bullet} \\
B & \bullet \arrow[r, Rightarrow] & \bullet \arrow[r, Rightarrow] \arrow[u, "g^y"'] & K_B \doteq (R_A)^y
\end{tikzcd}
$$

If $R_A = g^{z}$ and $R_B = g^{w}$
where the adversary chose z, w

then K_A, K_B available to adversary

Security goal: Key secrecy

This diagram cannot occur

$$\bullet \Longrightarrow \bullet \Longrightarrow \circ \Longrightarrow \circ \; K_A$$

$$\bullet \; K_A$$

Subject to assumptions, e.g.
x, y randomly chosen by compliant principal

Static DH

Certificate authority authenticates, signs cert:

$$c_P = [\![\, \text{cert } Y_P,\ P \,]\!]_{\text{CA}}$$

where $Y_A = g^a \quad Y_B = g^b$

$$\begin{tikzcd}
A & \bullet \arrow[r, Rightarrow] \arrow[d, "c_A"] & \bullet \arrow[r, Rightarrow] & K_A \doteq (Y_B)^a = g^{ba} \\
B & \bullet \arrow[r, Rightarrow] & \bullet \arrow[r, Rightarrow] \arrow[u, "c_B"'] & K_B \doteq (Y_A)^b = g^{ab}
\end{tikzcd}$$

Drawback: A, B get same K for every run!

Implicitly Authenticated DH

- Use both ephemeral and static (certified) values
- Ephemeral g^x, g^y ensure variation in key
- Static g^a, g^b ensure authenticity implicitly:

If any principal P has computed K
then either $P = A$ or $P = B$

Security goal: Implicit authentication

$$[A, B, \ldots] \qquad \bullet \Longrightarrow \bullet \Longrightarrow \circ \Longrightarrow \circ\ K$$

$$[B', A', \ldots] \qquad \bullet \Longrightarrow \bullet \Longrightarrow \circ \Longrightarrow \circ\ K$$

If *long term values* a, b *unknown to adversary*
then $A = A'$, $B = B'$

This paper

1. Gives equational theory of abelian groups with exponentiation:

   AGˆ *characterizes the equations* $s = t$
   that are uniformly valid as group varies

This paper

1. Gives equational theory of abelian groups with exponentiation:

   AGˆ *characterizes the equations* $s = t$
   that are uniformly valid as group varies

2. Formalizes implicitly authenticated Diffie-Hellman protocol behavior and adversary over Free(AGˆ)

This paper

1. Gives equational theory of abelian groups with exponentiation:

   AGˆ *characterizes the equations* $s = t$
   that are uniformly valid as group varies

2. Formalizes implicitly authenticated Diffie-Hellman protocol behavior and adversary over Free(AGˆ)
3. Shows indicator theorem:

   Occurrences of secret exponents do not change
   through adversary actions

This paper

1. Gives equational theory of abelian groups with exponentiation:

   AGˆ *characterizes the equations* $s = t$
   that are uniformly valid as group varies

2. Formalizes implicitly authenticated Diffie-Hellman protocol behavior and adversary over Free(AGˆ)
3. Shows indicator theorem:

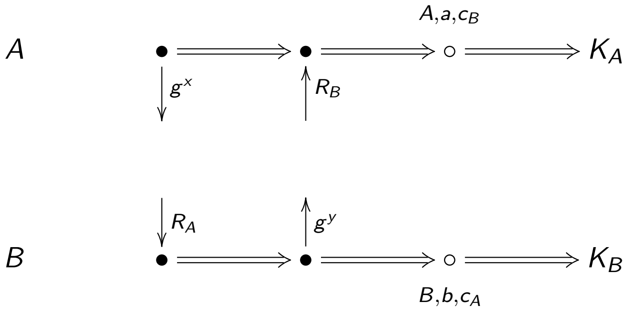
   Occurrences of secret exponents do not change
   through adversary actions

4. Shows security goals using indicator theorem

   Gives insights when they fail

IADH Protocols

$$c_A = [\![\, \text{cert } g^a,\ A \,]\!]_{\text{CA}} \qquad c_B = [\![\, \text{cert } g^b,\ B \,]\!]_{\text{CA}}$$



$$K_A = f(A, B, a, x, R_B, Y_B) \qquad K_B = f(A, B, b, y, R_A, Y_A)$$

Some IADH shared secret computations

Computation done by A

H($\cdot$) is a hash fn

$$K_{um} \quad = \quad \mathrm{H}({Y_B}^a, {R_B}^x) \quad \stackrel{?}{=} \qquad \mathrm{H}(g^{ab}, g^{xy})$$

Security goal: No impersonation

This diagram should be prevented

$$\bullet \Longrightarrow \bullet \Longrightarrow \circ \Longrightarrow \circ \; K_A$$

$$\bullet \; K_A$$

Your long term value b
and my ephemeral value x
unknown to adversary

$$K_A = \mathrm{H}(g^{ab}, g^{xy})$$

Some IADH shared secret computations

Computation done by A

$\mathrm{H}(\cdot)$ is a hash fn

$$
\begin{aligned}
K_{um} &= \mathrm{H}({Y_B}^a, {R_B}^x) &\stackrel{?}{=}& \quad \mathrm{H}(g^{ab}, g^{xy}) \\
K_{cf} &= (R_B Y_B)^{x+a} &\stackrel{?}{=}& \quad g^{(y+b)(x+a)} = g^{xy} g^{ay} g^{xb} g^{ab}
\end{aligned}
$$

Our central contribution

Formal theory and semantics in which
occurrences of variables in exponents
are a security invariant

Some IADH shared secret computations

Computation done by A

H($\cdot$) is a hash fn

$$
\begin{aligned}
K_{um} &= \mathrm{H}({Y_B}^a, {R_B}^x) &\stackrel{?}{=}& \quad \mathrm{H}(g^{ab}, g^{xy}) \\
K_{cf} &= (R_B Y_B)^{x+a} &\stackrel{?}{=}& \quad g^{(y+b)(x+a)} = g^{xy} g^{ay} g^{xb} g^{ab} \\
K_{\_\_qv} &= (R_B {Y_B}^E)^{x+Da} &\stackrel{?}{=}& \quad g^{xy} g^{Day} g^{xEb} g^{DEab}
\end{aligned}
$$

Some IADH shared secret computations

Computation done by A

$\mathrm{H}(\cdot)$ is a hash fn

$$
\begin{aligned}
K_{um} &= \mathrm{H}({Y_B}^a, {R_B}^x) &\overset{?}{=}& \quad \mathrm{H}(g^{ab}, g^{xy}) \\
K_{cf} &= (R_B Y_B)^{x+a} &\overset{?}{=}& \quad g^{(y+b)(x+a)} = g^{xy} g^{ay} g^{xb} g^{ab} \\
K_{\_\_qv} &= (R_B {Y_B}^E)^{x+Da} &\overset{?}{=}& \quad g^{xy} g^{Day} g^{xEb} g^{DEab}
\end{aligned}
$$

UM = "Unified model" CF = Cremers-Feltz

MQV: $E = [R_B], \quad D = [g^x]$

HMQV: $E = \mathrm{H}(R_B, B), \quad D = \mathrm{H}(g^x, A)$

AGˆ

1. $(G, \cdot, inv, id)$ is an abelian group;
2. $(E, +, 0, -, *, 1)$ is a commutative ring with identity;
3. Exponentiation makes G a right E-module with identity:

$$
\begin{array}{lll}
(a^x)^y = a^{x * y} & a^1 = a & id^x = id \\
(a \cdot b)^x = a^x \cdot b^x & & a^{(x+y)} = a^x \cdot a^y
\end{array}
$$

4. Multiplicative inverse, closure at sort NZE, subsort of E:

$$
\begin{array}{lll}
u ** v = u * v & u * i(u) = 1 & i(-u) = -i(u) \\
i(u * v) = i(u) * i(v) & i(1) = 1 & i(i(w)) = w
\end{array}
$$

Rewriting relation $\rightarrow_{AG\hat{}}$

Theorem

The reduction $\rightarrow_{AG\hat{}}$ is terminating

Verified with the Aprove termination tool

Theorem

The reduction $\rightarrow_{AG\hat{}}$ is confluent mod AC

Verified with the Maude Church-Rosser checker

Free(AGˆ) as a message algebra

- Regular principals run protocol with values from Free(AGˆ)
  - Free choices are fresh variables a, b, x, y
  - Message sent/received are Free(AGˆ) terms over them
  - Augmented with encryption, signature, hashing, etc

Free(AGˆ) as a message algebra

- Regular principals run protocol with values from Free(AGˆ)
  - Free choices are fresh variables a, b, x, y
  - Message sent/received are Free(AGˆ) terms over them
  - Augmented with encryption, signature, hashing, etc
- Adversary model: can apply operations of Σ(AGˆ)
  - May multiply, add, take inverses, ...
  - No logarithms (:-)
  - May also encrypt and decrypt with key, pair, unpair
  - May choose variables unless assumed fresh
- Messages s, t are equal if AGˆ entails $s = t$

Indicators relative to secret vars

Indicator of a monomial m counts occurrences of these vars in m:

$$\mathrm{Ind}_{\langle a,b,x,y\rangle}(ab) = \langle 1,1,0,0\rangle \qquad \mathrm{Ind}_{\langle a,b,x,y\rangle}(xy) = \langle 0,0,1,1\rangle$$

$$\mathrm{Ind}_{\langle b,x\rangle}(ab) = \langle 1,0\rangle \qquad \mathrm{Ind}_{\langle b,x\rangle}(xy) = \langle 0,1\rangle$$

Indicators relative to secret vars

Indicator of a monomial m counts occurrences of these vars in m:

$$\mathsf{Ind}_{\langle a,b,x,y\rangle}(ab) = \langle 1,1,0,0\rangle \qquad \mathsf{Ind}_{\langle a,b,x,y\rangle}(xy) = \langle 0,0,1,1\rangle$$

$$\mathsf{Ind}_{\langle b,x\rangle}(ab) = \langle 1,0\rangle \qquad \mathsf{Ind}_{\langle b,x\rangle}(xy) = \langle 0,1\rangle$$

Indicators of g^m singleton of indicator of m
Indicators of $t_1 \cdot t_2$ union of indicators of t_1 and t_2

Indicators relative to secret vars

Indicator of a monomial m counts occurrences of these vars in m:

$$\mathrm{Ind}_{\langle a,b,x,y\rangle}(ab) = \langle 1,1,0,0\rangle \qquad \mathrm{Ind}_{\langle a,b,x,y\rangle}(xy) = \langle 0,0,1,1\rangle$$

$$\mathrm{Ind}_{\langle b,x\rangle}(ab) = \langle 1,0\rangle \qquad \mathrm{Ind}_{\langle b,x\rangle}(xy) = \langle 0,1\rangle$$

Indicators of g^m singleton of indicator of m
Indicators of $t_1 \cdot t_2$ union of indicators of t_1 and t_2

$$\mathrm{Ind}_{\langle b,x\rangle}(g^{xy}g^{ay}g^{xb}g^{ab}) = \{\langle 0,1\rangle, \langle 1,1\rangle, \langle 1,0\rangle\}$$

Indicators relative to secret vars

Indicator of a monomial m counts occurrences of these vars in m:

$$\mathsf{Ind}_{\langle a,b,x,y\rangle}(ab) = \langle 1,1,0,0\rangle \qquad \mathsf{Ind}_{\langle a,b,x,y\rangle}(xy) = \langle 0,0,1,1\rangle$$

$$\mathsf{Ind}_{\langle b,x\rangle}(ab) = \langle 1,0\rangle \qquad \mathsf{Ind}_{\langle b,x\rangle}(xy) = \langle 0,1\rangle$$

Indicators of g^m singleton of indicator of m
Indicators of $t_1 \cdot t_2$ union of indicators of t_1 and t_2

$$\mathsf{Ind}_{\langle b,x\rangle}(g^{xy}g^{ay}g^{xb}g^{ab}) = \{\langle 0,1\rangle, \langle 1,1\rangle, \langle 1,0\rangle\}$$

Indicators of pairs union of indicators etc

$$\mathsf{Ind}_{\langle b,x\rangle}(\mathsf{H}(g^{ab}, g^{xy})) = \{\langle 1,0\rangle, \langle 0,1\rangle\}$$

IADH Regular Behavior

For any basis $\vec{v}$

If t is any message sent by any compliant IADH participant,
then $\mathrm{Ind}_{\vec{v}}(t)$ is a basis vector

$$\langle \vec{0}, 1, \vec{0} \rangle$$

The indicator theorem

Theorem

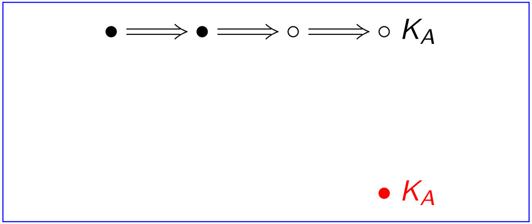
If the adversary can build t given messages S
then

$$\mathrm{Ind}_{\vec{v}}(t) \subseteq \bigcup_{s \in S} \mathrm{Ind}_{\vec{v}}(s) \cup \{\langle \vec{0} \rangle\}$$

when $\vec{v}$ is a list of secret NZE-variables

Security goal: Key secrecy

This diagram cannot occur in UM



$$K_A = \mathrm{H}(g^{ab}, {R_B}^{x})$$

Long term secrets a, b
uncompromised

Security goal: Key secrecy

This diagram cannot occur in UM

$$\bullet \Longrightarrow \bullet \Longrightarrow \circ \Longrightarrow \circ \; K_A$$

$$\bullet \; K_A$$

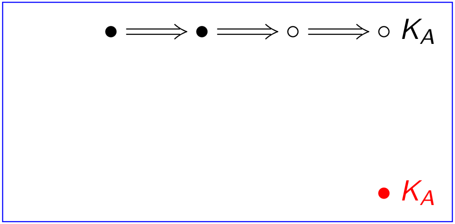
$$K_A = \mathsf{H}(g^{ab},\, {R_B}^{x})$$

Long term secrets a, b
uncompromised

$$\langle 1, 1\rangle \in \mathsf{Ind}_{\langle a,b\rangle}(\mathsf{H}(g^{ab},\, {R_B}^{x}))$$

Security goal: No impersonation

This diagram unfortunately can occur



$$K_A = \mathrm{H}(g^{ab}, g^{xy})$$

Where your b and my x remain secret

Security goal: No impersonation

This diagram unfortunately can occur

$$\bullet \Longrightarrow \bullet \Longrightarrow \circ \Longrightarrow \circ \; K_A$$

$$\bullet \; K_A$$

$$K_A = \mathsf{H}(g^{ab}, g^{xy})$$

Where your b and my x remain secret

$$\mathsf{Ind}_{\langle b,x \rangle}(\mathsf{H}(g^{ab}, g^{xy})) = \{\langle 1, 0 \rangle, \langle 0, 1 \rangle\}$$

semantics

Mathematical context

DH structures

G a cyclic group of prime order q

g a generator of G

set E of exponents $\{0, 1, \ldots, (q-1)\}$ forms a field: $\mathbb{F}_q$

Useful group presentations for crypto include subgroups of

$\mathbb{Z}_p^*$ the integers mod p

elliptic curve over a finite field

Mathematical context

hard problems

1. Discrete Logarithm problem:

   given g^x*, compute* x

2. Computational Diffie-Hellman problem:

   given $g^x, g^y \in G$*, compute* g^{xy}

3. Decisional Diffie-Hellman problem:

   given $g^x, g^y \in G$*, distinguish* g^{xy} *from random* g^z

Considered intractable in suitable groups

Mathematical context

hard problems

1. Discrete Logarithm problem:

   given g^x, compute x

2. Computational Diffie-Hellman problem:

   given $g^x, g^y \in G$, compute g^{xy}

3. Decisional Diffie-Hellman problem:

   given $g^x, g^y \in G$, distinguish g^{xy} from random g^z

Considered intractable in suitable groups
there is an infinite family of primes q s.t.
every PPT algorithm achieves advantage
only finitely often

Semantic requirement on AGˆ

- If $s = t$ valid for infinitely many q, adversary may use $s = t$
- Other tractable computations useful only in finitely many q

Semantic requirement on AGˆ

- If $s = t$ valid for infinitely many q, adversary may use $s = t$
- Other tractable computations useful only in finitely many q
- Equational completeness property:

$$\mathbb{F}_q \models s = t \text{ for infinitely many finite fields } \mathbb{F}_q$$

$$\text{implies}$$

$$\mathrm{AG\hat{}} \vdash s = t$$

Semantic requirement on AGˆ

- If $s = t$ valid for infinitely many q, adversary may use $s = t$
- Other tractable computations useful only in finitely many q
- Equational completeness property:

$$\mathbb{F}_q \models s = t \text{ for infinitely many finite fields } \mathbb{F}_q$$
$$\text{implies}$$
$$\mathrm{AG\hat{}} \vdash s = t$$

- Actually: $\mathbb{F}_q \models s = t$ infinitely often iff $\mathrm{AG\hat{}} \vdash s = t$

Models of AGˆ, 1

For any field F, define $\mathcal{M}_F$ such that $\mathcal{M}_F \models$ AGˆ:

E, G both interpreted as dom(F)

NZE interpreted as dom(F) $\setminus \{0\}$

Operations of E interpreted as in F itself

$\cdot, inv, id$ interpreted as $+_F$, $-_F$, 0

a^e interpreted as $a * e$

Models of AGˆ, 1

For any field F, define $\mathcal{M}_F$ such that $\mathcal{M}_F \models$ AGˆ:

E, G both interpreted as $\mathrm{dom}(F)$

NZE interpreted as $\mathrm{dom}(F) \setminus \{0\}$

Operations of E interpreted as in F itself

$\cdot, inv, id$ interpreted as $+_F$, $-_F$, 0

a^e interpreted as $a * e$

Some $\mathcal{M}_F$: When $F = \mathbb{F}_q$, we obtain $\mathcal{M}_q$
When $F = \mathbb{Q}$, we obtain $\mathcal{M}_{\mathbb{Q}}$

Models of AGˆ, 2

Let D be a non-principal ultrafilter over the prime numbers q

Write $\mathbb{F}_D$ for the ultraproduct

$$\prod_D \{\mathbb{F}_q \colon q \text{ prime}\}$$

Let $\mathcal{M}_D \models \text{AG}\hat{}$ be obtained from $\mathbb{F}_D$ as on last slide

Completeness of AGˆ for uniform equality

Theorem

For each pair of G-terms s and t, the following are equivalent

1. $\mathrm{AG\hat{}} \vdash s = t$
2. *For all q,* $\mathcal{M}_q \models s = t$
3. *For all non-principal D,* $\mathcal{M}_D \models s = t$
4. *For infinitely many q,* $\mathcal{M}_q \models s = t$
5. *For some non-principal D,* $\mathcal{M}_D \models s = t$
6. $\mathcal{M}_{\mathbb{Q}} \models s = t$
7. s, t *have the same normal form modulo AC*

This paper

1. Gives equational theory of abelian groups with exponentiation:
   - $\mathrm{AG}\hat{} \vdash s = t$ iff
     $\mathbb{F}_q \models s = t$ for infinitely many finite fields $\mathbb{F}_q$
   - Convergent associative-commutative rewriting system
   - Symbolic algebra Free(AGˆ) of normal forms
2. Formalizes implicitly authenticated Diffie-Hellman protocol behavior and adversary over Free(AGˆ)
3. Shows indicator theorem:

   Occurrences of secret exponents do not change through adversary actions

4. Shows security goals using indicator theorem

   Gives insights when they fail

A Handy Lemma about $\mathcal{M}_{\mathbb{Q}}$

Lemma

1. *$\mathcal{M}_{\mathbb{Q}}$ can be embedded as a submodel in any $\mathcal{M}_D$.*
2. *If s and t are distinct normal forms then $\mathcal{M}_{\mathbb{Q}} \not\models s = t$.*

Ultraproducts

D is an ultrafilter iff D is a maximal family of sets $\subseteq X$ such that:

- $\emptyset \notin D$
- $s_1, s_2 \in D$ implies $s_1 \cap s_2 \in D$
- $s_1 \in D$ and $s_1 \subseteq s_2$ implies $s_2 \in D$

D is principal iff $D = \{s \colon s_0 \subseteq s\}$ for some s_0

Ultraproduct $\prod_D \mathcal{M}_q$, for ultrafilter D:

let $\mathcal{M}_q$ be a family of structures indexed by $q \in X$
$\prod_D \mathcal{M}_q$ is a factored product such that

$$\prod_D \mathcal{M}_q \models \phi \quad \text{iff} \quad \{q \in X \colon \mathcal{M}_q \models \phi\} \in D$$

Ultraproducts

D is an ultrafilter iff D is a maximal family of sets $\subseteq X$ such that:

- $\emptyset \notin D$
- $s_1, s_2 \in D$ implies $s_1 \cap s_2 \in D$
- $s_1 \in D$ and $s_1 \subseteq s_2$ implies $s_2 \in D$

D is principal iff $D = \{s \colon s_0 \subseteq s\}$ for some s_0

Ultraproduct $\prod_D \mathcal{M}_q$, for ultrafilter D:

let $\mathcal{M}_q$ be a family of structures indexed by $q \in X$
$\prod_D \mathcal{M}_q$ is a factored product such that

$$\prod_D \mathcal{M}_q \models \phi \quad \text{iff} \quad \{q \in X \colon \mathcal{M}_q \models \phi\} \in D$$

Only consider non-principal ultrafilters