Intruder Deduction for the Equational Theory of *Exclusive-Or* with Commutative and Distributive Encryption

Pascal Lafourcade

SecRet'06

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

Venise, Italy****
15th July 2006

Symbolic approach

- Intruder controls the network
- Messages represented by terms
  - $\{m\}_k$
  - $\langle m_1, m_2 \rangle$
- Perfect encryption hypothesis

Symbolic approach

- Intruder controls the network
- Messages represented by terms
  - $\{m\}_k$
  - $\langle m_1, m_2 \rangle$
- Perfect encryption hypothesis

Advantages

- Automatic verification
- Useful abstraction

Symbolic approach

- Intruder controls the network
- Messages represented by terms
  - $\{m\}_k$
  - $\langle m_1, m_2 \rangle$
- Perfect encryption hypothesis $+$ algebraic properties

Advantages

- Automatic verification
- Useful abstraction

State of the Art

XOR : ACUN [Rusinowitch & al 03] [Comon-Shmatikov 03]

1. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
2. $x \oplus y = y \oplus x$ **C**ommutativity
3. $x \oplus 0 = x$ **U**nity
4. $x \oplus x = 0$ **N**ilpotency

ACUN and homomorphism [LLT05,Del 06] (AG)

$h(x \oplus y) = h(x) \oplus h(y)$

ACUN and distributive encryption [LLT06] (AG)

$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$

ACUN and distributive commutative encryption

$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$ and $\{\{x\}_{k_1}\}_{k_2} = \{\{x\}_{k_1}\}_{k_2}$

State of the Art

XOR : ACUN [Rusinowitch & al 03] [Comon-Shmatikov 03]

1. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
2. $x \oplus y = y \oplus x$ **C**ommutativity
3. $x \oplus 0 = x$ **U**nity
4. $x \oplus x = 0$ **N**ilpotency

ACUN and homomorphism [LLT05,Del 06] (AG)

$h(x \oplus y) = h(x) \oplus h(y)$

ACUN and distributive encryption [LLT06] (AG)

$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$

ACUN and distributive commutative encryption

$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$ and $\{\{x\}_{k_1}\}_{k_2} = \{\{x\}_{k_1}\}_{k_2}$

State of the Art

XOR : ACUN [Rusinowitch & al 03] [Comon-Shmatikov 03]

1. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
2. $x \oplus y = y \oplus x$ **C**ommutativity
3. $x \oplus 0 = x$ **U**nity
4. $x \oplus x = 0$ **N**ilpotency

ACUN and homomorphism [LLT05,Del 06] (AG)

$h(x \oplus y) = h(x) \oplus h(y)$

ACUN and distributive encryption [LLT06] (AG)

$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$

ACUN and distributive commutative encryption

$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$ and $\{\{x\}_{k_1}\}_{k_2} = \{\{x\}_{k_1}\}_{k_2}$

State of the Art

XOR : ACUN [Rusinowitch & al 03] [Comon-Shmatikov 03]

1. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
2. $x \oplus y = y \oplus x$ **C**ommutativity
3. $x \oplus 0 = x$ **U**nity
4. $x \oplus x = 0$ **N**ilpotency

ACUN and homomorphism [LLT05,Del 06] (AG)

$h(x \oplus y) = h(x) \oplus h(y)$

ACUN and distributive encryption [LLT06] (AG)

$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$

ACUN and distributive commutative encryption

$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$ and $\{\{x\}_{k_1}\}_{k_2} = \{\{x\}_{k_1}\}_{k_2}$

Outline

Outline

Extended Dolev-Yao Model

Deduction System:

$$(A)\ \frac{u \in T}{T \vdash u\downarrow}$$

$$(P)\ \frac{T \vdash u \qquad T \vdash v}{T \vdash \langle u, v\rangle\downarrow}$$

$$(C_K)\ \frac{T \vdash u \qquad T \vdash K}{T \vdash \{u\}_K\downarrow}$$

$$(D_K)\ \frac{T \vdash \{u\}_K \qquad T \vdash K}{T \vdash u\downarrow}$$

$$(UL)\ \frac{T \vdash \langle u, v\rangle}{T \vdash u\downarrow}$$

$$(UR)\ \frac{T \vdash \langle u, v\rangle}{T \vdash v\downarrow}$$

$$(GX)\ \frac{T \vdash u_1 \qquad \ldots \qquad T \vdash u_n}{T \vdash u_1 \oplus \ldots \oplus u_n\downarrow}$$

Special Rules Encryption and Decryption

(C_K) and (D_K)

$$(C_K) \quad \frac{T \vdash u \qquad T \vdash K}{T \vdash \{u\}_K\downarrow} \qquad\qquad (D_K) \quad \frac{T \vdash \{u\}_K \qquad T \vdash K}{T \vdash u\downarrow}$$

Where

- $K = \{k_1^{\alpha_1}, \ldots, k_n^{\alpha_n}\}$
- $T \vdash K$ is: $T \vdash k_1$ used α_1 times, $\ldots, T \vdash k_n$ used α_n times

Outline

Simple Proofs

simple proof

Each node $T \vdash v$ occurs at most once on each branch.

Cut the loops.

Simple and Flat Proofs

flat proof

Avoids two successive applications of the same rule : (C),(D) or (GX).

Merge rules (GX), (C) and (D).

Flat Transformations (I)

Rule (C)

$$(C_{K_2})\dfrac{(C_{K_1})\dfrac{T \vdash u \qquad T \vdash K_1}{T \vdash \{u\}_{K_1}\downarrow} \qquad T \vdash K_2}{T \vdash \{u\}_{K_1,K_2}}$$

$$\Downarrow$$

$$(C_{K_1,K_2})\dfrac{T \vdash u \qquad T \vdash K_1, K_2}{T \vdash \{u\}_{K_1,K_2}\downarrow}$$

Flat Transformations (II)

Rule (D)

$$(D_{K_2})\frac{(D_{K_1})\dfrac{T \vdash \{u\}_K \qquad T \vdash K_1}{T \vdash \{u\}_{K \setminus K_1}\downarrow} \qquad T \vdash K_2}{T \vdash \{u\}_{K \setminus (K_1, K_2)}}$$

$$\Downarrow$$

$$(D_{K_1,K_2})\frac{T \vdash u \qquad T \vdash K_1, K_2}{T \vdash \{u\}_{K \setminus (K_1, K_2)}\downarrow}$$

Flat Transformations (III)

Rule (GX)

$$(GX)\frac{(GX)\dfrac{T \vdash x_1 \quad \ldots \quad T \vdash x_n}{T \vdash x_1 \oplus \ldots \oplus x_n} \quad T \vdash y_1 \quad \ldots \quad T \vdash y_m}{T \vdash x_1 \oplus \ldots \oplus x_n \oplus y_1 \oplus \ldots \oplus y_m}$$

$$\Downarrow$$

$$(GX)\frac{T \vdash x_1 \quad \ldots \quad T \vdash x_n \quad T \vdash y_1 \quad \ldots \quad T \vdash y_m}{T \vdash x_1 \oplus \ldots \oplus x_n \oplus y_1 \oplus \ldots \oplus y_m}$$

D-eager Proof

D-eager proof = rules (D) applied as early as possible.

Definition

In *D-eager* proof these 2 cases are impossible :

$$(D_{K_2})\dfrac{(C_{K_1})\dfrac{\dfrac{\vdots}{T \vdash u} \quad \dfrac{\vdots}{T \vdash K_1}}{T \vdash \{u\}_{K_1}} \qquad \dfrac{\vdots}{T \vdash K_2}}{\{u\}_{K_1 \setminus K_2}}$$

D-eager Proof

D-eager proof = rules (D) applied as early as possible.

Definition

In *D-eager* proof these 2 cases are impossible :

$$(D_{K_2})\frac{(C_{K_1})\dfrac{\dfrac{\vdots}{T \vdash u} \quad \dfrac{\vdots}{T \vdash K_1}}{T \vdash \{u\}_{K_1}} \qquad \dfrac{\vdots}{T \vdash K_2}}{\{u\}_{K_1 \setminus K_2}}$$

$K_2 \cap K_1 \neq \emptyset$

$$(D_{K_2})\frac{(GX)\dfrac{(R_1)\dfrac{\vdots}{T \vdash \{u_1\}_{K_1}} \quad \ldots \quad (R_n)\dfrac{\vdots}{T \vdash u_n}}{T \vdash \{u\}_{K_2}} \quad T \vdash K_2}{T \vdash u}$$

D-eager Transformations (I)

Rule (C) and (D) are commutative

Consequence of simplicity, $K_1 \cap K_2 = \emptyset$.

$$(D_{K_2})\dfrac{(C_{K_1})\dfrac{\dfrac{\vdots}{T \vdash \{u\}_K} \quad \dfrac{\vdots}{T \vdash K_1}}{T \vdash \{u\}_{K,K_1}} \quad \dfrac{\vdots}{T \vdash K_2}}{\{u\}_{(K,K_1)\setminus K_2}}$$

Is equivalent to

$$(C_{K_1})\dfrac{(D_{K_2})\dfrac{\dfrac{\vdots}{T \vdash \{u\}_K} \quad \dfrac{\vdots}{T \vdash K_2}}{T \vdash \{u\}_{K\setminus K_2}} \quad \dfrac{\vdots}{T \vdash K_1}}{\{u\}_{(K\setminus K_2),K_1} = \{u\}_{(K,K_1)\setminus K_2}}$$

D-eager Transformation (II)

if $K_2 \cap K_1 \neq \emptyset$

$$
(D_{K_2})\dfrac{(GX)\dfrac{(R_1)\dfrac{\vdots}{T \vdash \{B_1\}_{K_1}} \quad (R_2)\dfrac{\vdots}{T \vdash B_2} \quad \dots \quad (R_n)\dfrac{\vdots}{T \vdash B_n}}{T \vdash \{u\}_{K_1}} \quad T \vdash K_2}{T \vdash \{u\}_{K_1 \setminus K_2}}
$$

$$\Downarrow$$

$$
(D_{K_2 \setminus K_1})\dfrac{(GX)\dfrac{(D_{K_2 \cap K_1})\dfrac{T \vdash \{B_1\}_{K_1} \quad T \vdash K_1 \setminus K_2 \cap K_1}{T \vdash \{B_1\}_{(K1 \setminus K_2 \cap K_1)}} \quad \dots \quad (D_{K_2 \cap K_1})\dfrac{(GX)\dfrac{(R_2)\dfrac{\vdots}{T \vdash B_2} \quad \dots \quad (R_n)\dfrac{\vdots}{T \vdash B_n}}{T \vdash \{u_l\}_{K_1}} \quad T \vdash K_2 \cap K_1}{T \vdash \{u_1\}_{(K_1 \setminus K_2 \cap K_1)}}}{T \vdash \{u\}_{(K_1 \setminus K_2 \cap K_1)}} \quad T \vdash K_2 \setminus K_1}{T \vdash \{u\}_{(K_1 \setminus K_2 \cap K_1) \setminus (K_2 \setminus K_1)} = \{u\}_{K_1 \setminus K_2}}
$$

$\oplus$-*eager* Proofs

$\oplus$-*eager* proof = rules (GX) applied as early as possible.

Definition

A $\oplus$-*eager* proof authorizes only :

$$(GX)\dfrac{(C_{K_1})\dfrac{T \vdash x_1 \quad T \vdash K_1}{T \vdash \{x_1\}_{K_1}} (C_{K_2})\dfrac{T \vdash x_2 \quad T \vdash K_2}{T \vdash \{x_2\}_{K_2}} (R_1)\dfrac{\vdots}{T \vdash z_1} \ldots (R_m)\dfrac{\vdots}{T \vdash z_m}}{T \vdash \{x_1\}_{K_1} \oplus \{x_2\}_{K_2} \oplus z_1 \oplus \ldots \oplus z_m}$$

with $K_1 \cap K_2 \neq \emptyset$

$\oplus$-*eager* Transformation

Switch (GX) and (C), if $K_1 \cap K_2 \neq \emptyset$

$$(GX)\frac{(C_{K_1})\dfrac{T \vdash x_1 \qquad T \vdash K_1}{T \vdash \{x_1\}_{K_1}} \quad (C_{K_2})\dfrac{T \vdash x_2 \qquad T \vdash K_2}{T \vdash \{x_2\}_{K_2}}}{T \vdash \{x_1\}_{K_1} \oplus \{x_2\}_{K_2}}$$

$$K_1 \cap K_2 \neq \emptyset$$

$$\Downarrow$$

$$(GX)\frac{(C_{K_1 \cap K_2})\dfrac{(GX)\dfrac{(C_{K_1 \setminus K_2})\dfrac{T \vdash x_1 \qquad T \vdash K_1 \setminus K_2}{T \vdash \{x_1\}_{K_1 \setminus K_2}} \quad (C_{K_2 \setminus K_1})\dfrac{T \vdash x_2 \qquad T \vdash K_2 \setminus K_1}{T \vdash \{x_2\}_{K_2 \setminus K_1}}}{T \vdash \{x_1\}_{K_1 \setminus K_2} \oplus \{x_2\}_{K_2 \setminus K_1}} \qquad T \vdash K_1 \cap K_2}{T \vdash \{x_1\}_{K_1} \oplus \{x_2\}_{K_2}}}{T \vdash \{x_1\}_{K_1} \oplus \{x_2\}_{K_2}}$$

Outline

Main Theorem

The intruder deduction problem for a commutative and distributive encryption over XOR is decidable in 2-EXP-TIME.

Proof :
Using usual MacAllester approach :

- Locality Lemma
- $S_{\oplus}(T)$ computable in 2-EXP-TIME
- One-step deducibility in PTIME (solving linear equations)

Subterms

Definition

The set of *subterms* of a term t is the smallest set $S_T(t)$ s.t.:

- $t \in S_T(t)$.
- if $\langle u, v \rangle \in S_T(t)$ then $u, v \in S_T(t)$.
- if $\{u\}_K \in S_T(t)$ and $K = \{k_1^{\alpha_1}, \ldots, k_p^{\alpha_p}\}$ then $u \in S_T(t)$ and $k_i \in S_T(t)$ for all i $1 \leq i \leq p$.
- if $u = u_1 \oplus \ldots \oplus u_n \in S_T(t)$ then all $u_i \subseteq S_T(t)$.
- If $n > 1$, $K = \{k_1^{\alpha_1}, \ldots, k_p^{\alpha_p}\}$ and $\{u_1\}_K \oplus \ldots \oplus \{u_n\}_K \in S_T(t)$ then $u_1 \oplus \ldots \oplus u_n \in S_T(t)$.

Subterms

Definition

The set of *subterms* of a term t is the smallest set $S_T(t)$ s.t.:

- $t \in S_T(t)$.
- if $\langle u, v \rangle \in S_T(t)$ then $u, v \in S_T(t)$.
- if $\{u\}_K \in S_T(t)$ and $K = \{k_1^{\alpha_1}, \ldots, k_p^{\alpha_p}\}$ then $u \in S_T(t)$ and $k_i \in S_T(t)$ for all i $1 \leq i \leq p$.
- if $u = u_1 \oplus \ldots \oplus u_n \in S_T(t)$ then all $u_i \subseteq S_T(t)$.
- If $n > 1$, $K = \{k_1^{\alpha_1}, \ldots, k_p^{\alpha_p}\}$ and $\{u_1\}_K \oplus \ldots \oplus \{u_n\}_K \in S_T(t)$ then $u_1 \oplus \ldots \oplus u_n \in S_T(t)$.

Example : $u = \{a\}_{k1,k2,k3}$ then $S_T(u) =$
$\{u, a, k_1, k_2, k_3, \{a\}_{k1}, \{a\}_{k2}, \{a\}_{k3}, \{a\}_{k1,k2}, \{a\}_{k2,k3}, \{a\}_{k1,k3}\}$

Subterms

Definition

The set of *subterms* of a term t is the smallest set $S_T(t)$ s.t.:

- $t \in S_T(t)$.
- if $\langle u, v \rangle \in S_T(t)$ then $u, v \in S_T(t)$.
- if $\{u\}_K \in S_T(t)$ and $K = \{k_1^{\alpha_1}, \dots, k_p^{\alpha_p}\}$ then $u \in S_T(t)$ and $k_i \in S_T(t)$ for all i $1 \leq i \leq p$.
- if $u = u_1 \oplus \dots \oplus u_n \in S_T(t)$ then all $u_i \subseteq S_T(t)$.
- If $n > 1$, $K = \{k_1^{\alpha_1}, \dots, k_p^{\alpha_p}\}$ and $\{u_1\}_K \oplus \dots \oplus \{u_n\}_K \in S_T(t)$ then $u_1 \oplus \dots \oplus u_n \in S_T(t)$.

Example : $u = \{a\}_{k1,k2,k3}$ then $S_T(u) = \{u, a, k_1, k_2, k_3, \{a\}_{k1}, \{a\}_{k2}, \{a\}_{k3}, \{a\}_{k1,k2}, \{a\}_{k2,k3}, \{a\}_{k1,k3}\}$

$$S_{\oplus}(T) := \left\{ (\bigoplus_{s \in M} s)\downarrow \mid M \subseteq S_T(T) \right\}$$

Subterms

Definition

The set of *subterms* of a term t is the smallest set $S_T(t)$ s.t.:

- $t \in S_T(t)$.
- if $\langle u, v\rangle \in S_T(t)$ then $u, v \in S_T(t)$.
- if $\{u\}_K \in S_T(t)$ and $K = \{k_1^{\alpha_1}, \dots, k_p^{\alpha_p}\}$ then $u \in S_T(t)$ and $k_i \in S_T(t)$ for all i $1 \leq i \leq p$.
- if $u = u_1 \oplus \dots \oplus u_n \in S_T(t)$ then all $u_i \subseteq S_T(t)$.
- If $n > 1$, $K = \{k_1^{\alpha_1}, \dots, k_p^{\alpha_p}\}$ and $\{u_1\}_K \oplus \dots \oplus \{u_n\}_K \in S_T(t)$ then $u_1 \oplus \dots \oplus u_n \in S_T(t)$.

Example : $u = \{a\}_{k1,k2,k3}$ then $S_T(u) = \{u, a, k_1, k_2, k_3, \{a\}_{k1}, \{a\}_{k2}, \{a\}_{k3}, \{a\}_{k1,k2}, \{a\}_{k2,k3}, \{a\}_{k1,k3}\}$

$$S_\oplus(T) := \left\{ (\bigoplus_{s \in M} s)\downarrow \mid M \subseteq S_T(T) \right\}$$ 2-EXP-TIME

Idea of our approach (I)

Lemma

P a minimal proof in number of nodes $\Rightarrow$ P is S. F.

Idea of our approach (I)

Lemma

P a minimal proof in number of nodes $\Rightarrow$ P is S. F.

Let P be a proof of $T \vdash w$

1. From a proof to S. F. proof
2. From S. F. proof to S. F. *D-eager* proof
3. From S. F. *D-eager* proof to S. F. $\oplus$*-eager* and *D-eager* proof

Idea of our approach (II)

Lemma (D)

Let P be a Simple Flat *D-eager* and *$\oplus$-eager* proof of $T \vdash w$ if P is

$$(D_K)\dfrac{(R)\dfrac{\vdots}{T \vdash \{u\}_K\downarrow = r} \qquad \dfrac{\vdots}{T \vdash K\downarrow}}{T \vdash u}$$

then $\{u\}_K \in S_{\oplus}(T)$.

Proof of Lemma(D)

$$
(D_K)\dfrac{(GX)\dfrac{(R_1)\dfrac{T \vdash B_1}{T \vdash B_1'} \quad \ldots \quad (R_n)\dfrac{T \vdash B_n}{T \vdash B_n'}}{T \vdash \{u\}_K\downarrow} \qquad \dfrac{\vdots}{T \vdash K\downarrow}}{T \vdash u\downarrow}
$$

If $(R_1) = (C_{K'})$ use to prove that all $B_i' \in S_{\oplus}(T)$:

- $B_1' = \{B_1\}_{K'}$
- D-*eager* $\Rightarrow K \cap K' = \emptyset$
- $\oplus$-*eager* $\Rightarrow$ no rule $(R_j) = (C_{K''})$ s.t. $K'' \cap K = \emptyset$

Intruder Deduction Problem

Locality Lemma

A Simple Flat *D-eager* and $\oplus$*-eager* proof of $T \vdash w$ is a $S_{\oplus}(T, w)$-local proof.

Main Theorem

The intruder deduction problem for a commutative and distributive encryption over XOR is decidable in 2-EXP-TIME.

Proof :

Using usual MacAllester approach :

- Locality Lemma
- $S_{\oplus}(T)$ computable in 2-EXP-TIME
- One-step deducibility in PTIME (solving linear equations)

Outline

Definitions

Binary proof

All nodes of P with $\oplus$ are of the form $* \oplus *$

- Asymmetric encryption

$$(D_K)\frac{T \vdash \{u\}_K \qquad T \vdash Inv(K)}{T \vdash u\!\downarrow}$$

- Notation $\{\{u\}_{k_1}\}_{k_2}$ by $\{u\}_{k_1 k_2}$
- Uniform word problem in commutative semi-groups *(CSG)* is EXP-SPACE hard [Mayr Meyer 82].

Result

Result

In binary case the intruder deduction is EXP-SPACE-hard.

Remark : Assume not *Inv* symbol in T $\Rightarrow$ only rule (C) and (GX)

Transformation

$$(C_K)\frac{(GX)\dfrac{T \vdash x_1 \ldots T \vdash x_1}{T \vdash x_1 \oplus \ldots \oplus x_n} \quad T \vdash K}{T \vdash \{x_1\}_K \oplus \ldots \oplus \{x_n\}_K}$$

gives

$$(GX)\frac{(C_K)\dfrac{T \vdash x_1 \;\; T \vdash K}{T \vdash \{x_1\}_K} \ldots (C_K)\dfrac{T \vdash x_n \;\; T \vdash K}{T \vdash \{x_n\}_K}}{T \vdash \{x_1\}_K \oplus \ldots \oplus \{x_n\}_K}$$

Idea of the Proof

$$
\dfrac{
\dfrac{\dfrac{\dfrac{\{\circledast\}_{\gamma_1} \oplus \{\circledast\}_{\delta_1} \in T}{T \vdash \{\circledast\}_{\gamma_1} \oplus \{\circledast\}_{\delta_1}}(A)}{\vdots}(C)}{T \vdash \{\circledast\}_{\gamma_1 c_1} \oplus \{\circledast\}_{\delta_1 c_1}}(C)
\quad \cdots \quad
\dfrac{\dfrac{\dfrac{\{\circledast\}_{\gamma_l} \oplus \{\circledast\}_{\delta_l} \in T}{T \vdash \{\circledast\}_{\gamma_l} \oplus \{\circledast\}_{\delta_l}}(A)}{\vdots}(C)}{T \vdash \{\circledast\}_{\gamma_l c_l} \oplus \{\circledast\}_{\delta_l c_l}}(C)
}{T \vdash \{\circledast\}_{\alpha} \oplus \{\circledast\}_{\beta}}(GX)
$$

An instance of uniform word problem in CSG is:

$$\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n \models \alpha = \beta$$

Chose :

$\alpha =_C \gamma_1 c_1, \quad \delta_1 c_1 =_c \gamma_2 c_2, \quad \ldots \quad \delta_{l-1} c_{l-1} =_C \gamma_l c_l, \quad \delta_l c_l =_C \beta$

Outline

Results & Future Works

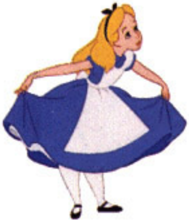
Results

- Solve Intruder deduction problem in 2-EXP-TIME
- In binary case a precise complexity.

Future Works

- Extension : **AG** and distributive, commutative encryption
- **Active Intruder** for ACUN and distributive encryption

Thank you for your attention



Questions ?