

A research paper by M. Abadi and P. Rogaway

Reconciling Two Views of Cryptography

Oral presentation: *Jérôme Javelle*, Violaine Juillard, *Guillaume Mangeot*,
Loic Ripert and Stéphane Wloka

Introduction

- First : The formal view
- Second : The computational view
- The goal : formal \approx computational

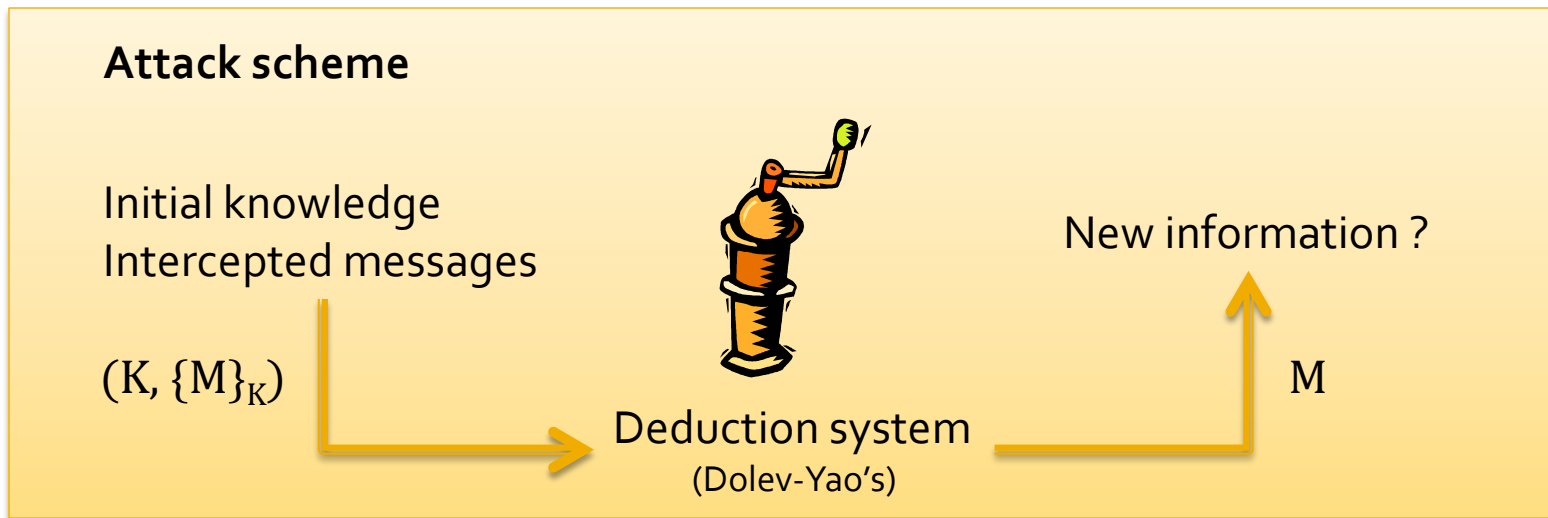
Outline

Reconciling Two Views of Cryptography

- Introduction
- The formal view
- The computational view
- Reconciliation
- Conclusion

The formal view (1/3)

- Focus on message structure
- Exchanged messages are expressions:
 - A bit stream in clear M or an encryption key K
 - A pair of expressions (M, N)
 - An encrypted expression $\{M\}_K$



The formal view (2/3)

- A pattern : visibility of an intruder
 - A bit stream in clear M or an encryption key K
 - A pair of patterns (M, N)
 - An encrypted pattern $\{M\}_K$
 - Something undecipherable \square
 - Extract a pattern from an expression:
 1. List the deducible keys:
 $(K_1, \{K_2\}_{K_1}, \{M\}_{K_3}) \vdash (K_1, K_2)$
 2. Retrieve a pattern with them:
 $pattern((K_1, \{K_2\}_{K_1}, \{M\}_{K_3})) = (K_1, \{K_2\}_{K_1}, \square)$
- } Same for an expression

The formal view (3/3)

- Equivalence relation:

$$M \equiv N \Leftrightarrow \text{pattern}(M) = \text{pattern}(N)$$

- $(K_1, \{K_2\}_{K_1}, \{M\}_{K_3}) \equiv (K_1, \{K_2\}_{K_1}, \{N\}_{K_4})$
- $(K_1, \{K_2\}_{K_1}, \{M\}_{K_3}) \cong (K_2, \{K_1\}_{K_2}, \{N\}_{K_4})$

Equivalence up to key renaming

- Close to indistinguishability from computational view

Outline

Reconciling Two Views of Cryptography

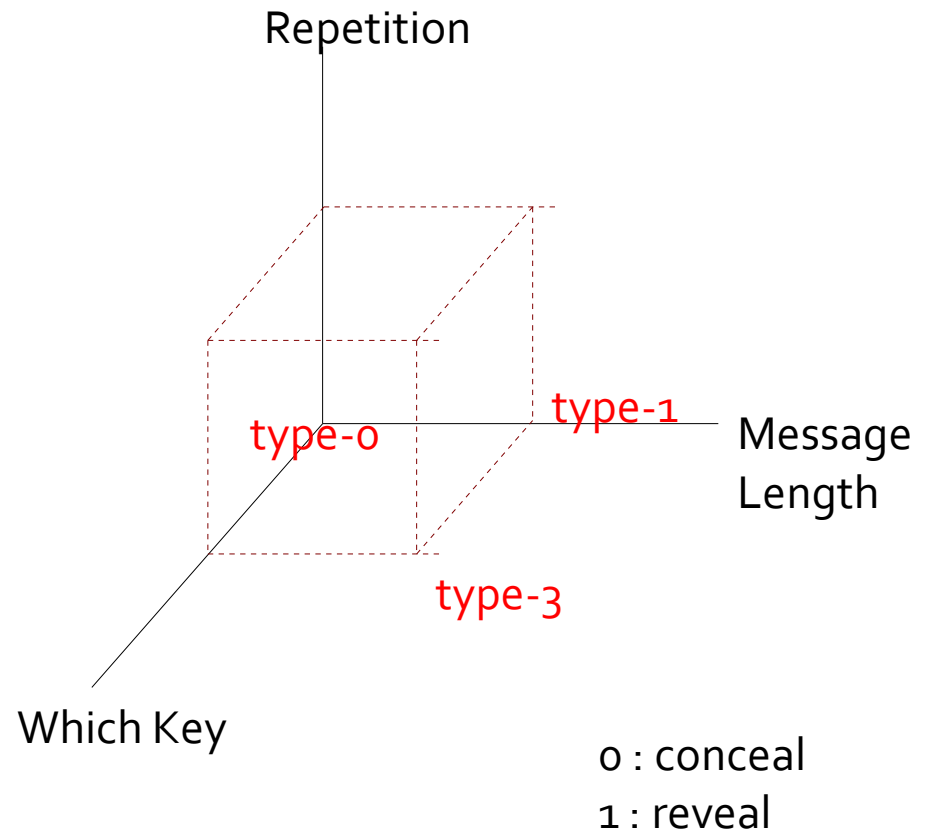
- Introduction
- The formal view
- The computational view
- Reconciliation
- Conclusion

The computational view (1/3)

- Consider messages as suite of bits
(String = $\{1,0\}^*$)
 - Sets of finite strings
- Probabilistic polynomial time algorithms
 - Adversary is a Turing Machine

The computational view (2/3)

- Attributes to conceal / reveal
 - **Repetition** : 2 different encryptions of m does not outputs the same cipher
 - **Which key** : There is no indication of the key used for encryption
 - **Message length** : One can not deduce length of plaintext
- Defines security types
 - type-0 .. type-7



The computational view (3/3)

- Indistinguishability ($D \approx D'$)
 - $e(\eta) = \Pr[x \leftarrow D\eta : A(\eta, x) = 1] - \Pr[x \leftarrow D'\eta : A(\eta, x) = 1]$ is negligible
- Security types advantages:
 - Type 3:

$$\Pr[k \leftarrow K(\eta) : A^{Ek(\cdot)}(\eta) = 1] - \Pr[k \leftarrow K(\eta) : A^{Ek(0|\cdot)}(\eta) = 1]$$
 - Type 1:

$$\Pr[k, k' \leftarrow K(\eta) : A^{Ek(\cdot), Ek'(\cdot)}(\eta) = 1] - \Pr[k \leftarrow K(\eta) : A^{Ek(0|\cdot), Ek(0|\cdot)}(\eta) = 1]$$
 - Type 0:

$$\Pr[k, k' \leftarrow K(\eta) : A^{Ek(\cdot), Ek'(\cdot)}(\eta) = 1] - \Pr[k \leftarrow K(\eta) : A^{Ek(0), Ek(0)}(\eta) = 1]$$

Outline

Reconciling Two Views of Cryptography

- Introduction
- The formal view
- The computational view
- Reconciliation
- Conclusion

Reconciliation (1/6)

Motivations

- Different abstraction levels
- Equivalence implies **indistinguishability**
 - Two equivalent expressions $M \cong N$
 - **Type-0 security** encryption scheme
 - Craft a **string** $\llbracket M \rrbracket$ from an **expression** M
 - **Indistinguishable** strings $\llbracket M \rrbracket \approx \llbracket N \rrbracket$

Formal view
Computational view

Reconciliation (2/6)

Key ordering

- Find recoverable and hidden keys of an expression
- Sort the hidden keys according to their accessibility
- To finish rewrite the expression

- Example :

- $M = \{0\}_{K_6} \{K_1 \ 1\}_{K_4} K_2 \{0\}_{K_3} \{K_6\}_{K_4} \{K_1 \ K_3\}_{K_4} \{1 \ 1 \ 1\}_{K_5} 0 \{K_1\}_{K_6} \{K_5\}_{K_2}$

- recoverable(M) are $\{K_2, K_5\} \rightarrow \{J_1, J_2\}$

- hidden(M) are $\{K_1, K_3, K_4, K_6\} \rightarrow \{K_1, K_2, K_4, K_3\}$

- New expression M' :

$$\{0\}_{K_3} \{K_1 \ 1\}_{K_4} J_1 \{0\}_{K_2} \{K_3\}_{K_4} \{K_1 \ K_2\}_{K_4} \{1 \ 1 \ 1\}_{J_2} 0 \{K_1\}_{K_3} \{J_2\}_{J_1}$$

Reconciliation (3/6)

Hybrid patterns

- Starting points: $M_0 = \text{pattern}(M')$ and $N_0 = \text{pattern}(N')$
- Successively add ordered keys:

M'										
M_4 :	$\{0\}_{K_3}$	$\{K_1 1\}_{K_4}$	J_1	$\{0\}_{K_2}$	$\{K_3\}_{K_4}$	$\{K_1 K_2\}_{K_4}$	$\{111\}_{J_2}$	0	$\{K_1\}_{K_3}$	$\{J_2\}_{J_1}$
M_3 :	$\{0\}_{K_3}$	□	J_1	$\{0\}_{K_2}$	□	□	$\{111\}_{J_2}$	0	$\{K_1\}_{K_3}$	$\{J_2\}_{J_1}$
M_2 :	□	□	J_1	$\{0\}_{K_2}$	□	□	$\{111\}_{J_2}$	0	□	$\{J_2\}_{J_1}$
M_1 :	□	□	J_1	□	□	□	$\{111\}_{J_2}$	0	□	$\{J_2\}_{J_1}$
M_0 :	□	□	J_1	□	□	□	$\{111\}_{J_2}$	0	□	$\{J_2\}_{J_1}$
N_0 :	□	□	J_1	□	□	□	$\{111\}_{J_2}$	0	□	$\{J_2\}_{J_1}$
N_1 :	□	□	J_1	□	□	$\{1\}_{K_1}$	$\{111\}_{J_2}$	0	□	$\{J_2\}_{J_1}$
N_2 :	□	□	J_1	□	□	$\{1\}_{K_1}$	$\{111\}_{J_2}$	0	$\{0 0\}_{K_2}$	$\{J_2\}_{J_1}$
N_3 :	$\{1 1\}_{K_3}$	$\{J_2\}_{K_3}$	J_1	$\{J_2\}_{K_3}$	$\{K_2\}_{K_3}$	$\{1\}_{K_1}$	$\{111\}_{J_2}$	0	$\{0 0\}_{K_2}$	$\{J_2\}_{J_1}$
N'										

Reconciliation (4/6)

Hybrid patterns

- When pattern \square is recognized \rightarrow returns encryption of o with a specific key
 - Relies to type- o security
 - Repetition, Which-Key, Message Length
- Changes only in indexing the keys
 - $\rightarrow \llbracket M \rrbracket = \llbracket M' \rrbracket$
 - The goal is to prove $\llbracket M' \rrbracket \approx \llbracket N' \rrbracket$

Reconciliation (5/6)

Building an adversary

- Proceed by contradiction
- Polynomial time adversary:
 - $\lambda(\eta) = \Pr[y \leftarrow \llbracket M \rrbracket : A(\eta, y) = 1] - \Pr[y \leftarrow \llbracket N \rrbracket : A(\eta, y) = 1]$
not negligible
- Define:
 - $p_i(\eta) = \Pr[y \leftarrow \llbracket M_i \rrbracket : A(\eta, y) = 1]$
 - $q_i(\eta) = \Pr[y \leftarrow \llbracket N_i \rrbracket : A(\eta, y) = 1]$
- Then:
 - $\lambda = (p_m - p_{m-1}) + \dots + (p_1 - p_0) + (q_0 - q_1) + \dots + (q_{m-1} - q_m)$
- Triangle inequality: $\exists i / p_i - p_{i-1} \geq \lambda / (m + n)$

Reconciliation (6/6)

Building an adversary

- Given: $p_i - p_{i-1} \geq \lambda / (m + n)$
 - An adversary that distinguishes $\llbracket M_i \rrbracket$ from $\llbracket M_{i-1} \rrbracket$
 - Build an adversary that violates o-type security (contradiction)

$$\begin{array}{l}
 M' \\
 \parallel \\
 M_4: \{0\}_{K_3} \quad \{K_1 1\}_{K_4} \quad J_1 \quad \{0\}_{K_2} \quad \{K_3\}_{K_4} \quad \{K_1 K_2\}_{K_4} \quad \{111\}_{J_2} \quad 0 \quad \{K_1\}_{K_3} \quad \{J_2\}_{J_1} \\
 M_3: \{0\}_{K_3} \quad \square \quad J_1 \quad \{0\}_{K_2} \quad \square \quad \square \quad \{111\}_{J_2} \quad 0 \quad \{K_1\}_{K_3} \quad \{J_2\}_{J_1} \\
 M_2: \square \quad \square \quad J_1 \quad \{0\}_{K_2} \quad \square \quad \square \quad \{111\}_{J_2} \quad 0 \quad \square \quad \{J_2\}_{J_1} \\
 M_1: \square \quad \square \quad J_1 \quad \square \quad \square \quad \square \quad \{111\}_{J_2} \quad 0 \quad \square \quad \{J_2\}_{J_1} \\
 M_0: \square \quad \square \quad J_1 \quad \square \quad \square \quad \square \quad \{111\}_{J_2} \quad 0 \quad \square \quad \{J_2\}_{J_1}
 \end{array}$$

- Equivalence \implies Indistinguishability
- No converse
 - Ex: $(K, \{0\}_K)$ and $(K, \{1\}_K)$

Outline

Reconciling Two Views of Cryptography

- Introduction
- The formal view
- The computational view
- Reconciliation
- Conclusion

Conclusion

- Reminder of two worlds
- Concepts from formal view can be verified in computational view

Thank you for your attention

Reconciling Two Views of Cryptography

Questions ?