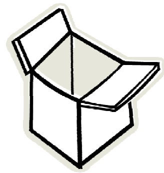
Department of Electrical Engineering – ESAT
KATHOLIEKE UNIVERSITEIT LEUVEN

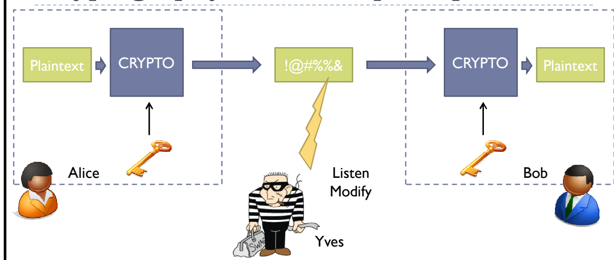


White-Box Cryptography

Ph.D graduation presentation
Brecht Wyseur

March 5, 2009, Heverlee

Cryptography: the basic principle

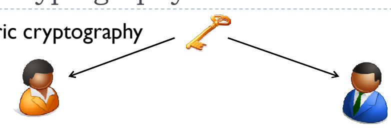


- Basic assumption
  - Adversary has knowledge of the algorithm (Kerckhoffs 1883 [104])
  - → Security of a cryptosystem system relies on the confidentiality of the key

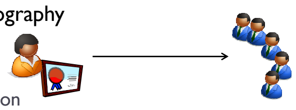
2

Keys in cryptography

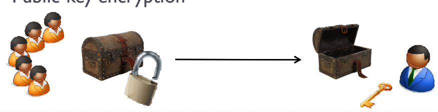
- Symmetric cryptography



- Asymmetric cryptography
  - Digital signatures



  - Public-key encryption



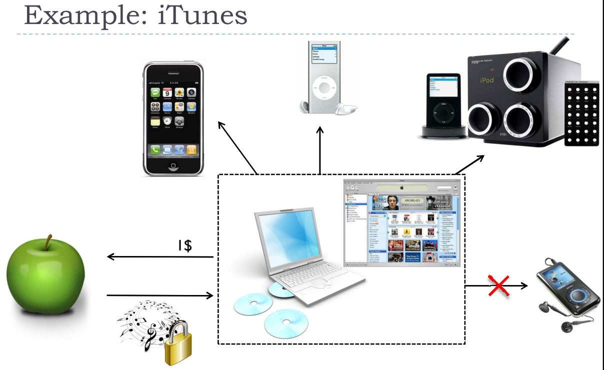
3

Cryptography is part of our modern life

- Telecommunication
- Financial
- Transport
- Identification
- Recreational
- …

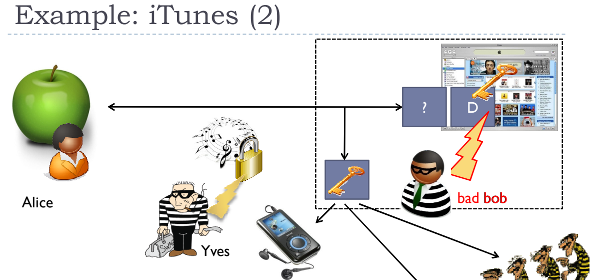
4

Example: iTunes



5

Example: iTunes (2)



- User has an incentive to attack the software
  - Break the restrictions posed on content
  - To steal protected data
  - To cheat (e.g., in an online game; access control)

6

Software Attacks

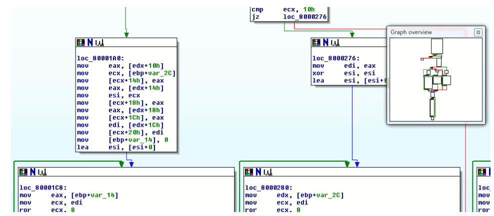
- When a user has an incentive to attack
- Or is subject to malware

- White-box attack model
  - Adversary has fully-privileged access to the execution platform
  - Dynamic execution (with instantiated cryptographic keys) can be observed,
  - Internal details of implementations are completely visible and alterable at will.

7

Software attacks

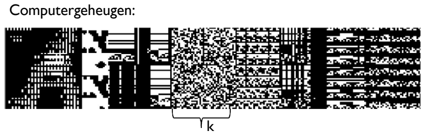
- Reverse engineering: attempt to decompile or understand binary code
  - Tools: IDA Pro, OllyDbg, Syser, Objdump, …



8

Entropy Attack (Shamir and Van Someren, 1999, [167])

Computergeheugen:



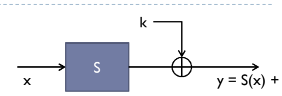
■ 0-bit
□ 1-bit

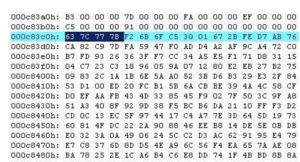
- Keys need to be chosen at random from a (uniform) distribution → high entropy.
- Code typically contains structure → low entropy

9

Key Whitening Attack (Kerins and Kursawe, 2006 [104])

- Implementation attack on ciphers that deploy a key-whitening (e.g., AES)





- Strategy: identify and overwrite S-box definition in binary:

  S → 0, then

  y = 0 + k

10

Digital Rights Management (DRM)

- Digital management of rights (/restrictions)
  - Audio, video, software (including games), education material, etc.
- IFPI
  - Global digital revenues by industry (2008)

Games	35%
Recorded Music	20%
Newspapers	4%
Films	4%
Magazines	1%

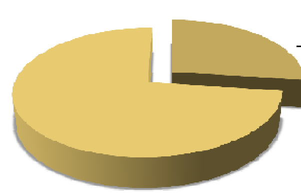
  - Digital music: €3 billion in trade value

GTA IV – 1000 developers for 3.5 years
Estimate production cost: €80 million

11

Software Piracy

- Illegal copy and distribution of software
- Business Software Alliance (BSA) (2006)

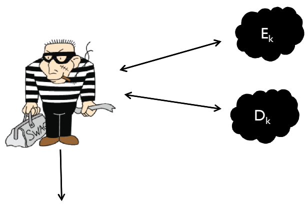


Belgium: 27% pirate SW
- 35% word-wide
- 82% in China

12

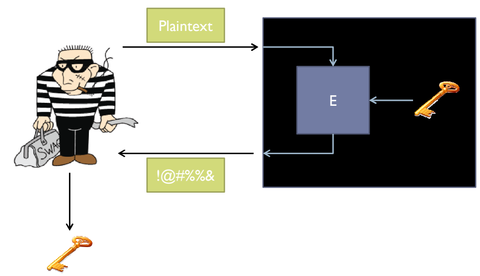
Traditional Assessment of Security

- Model of the *active* adversary:
  - Interaction with key-instantiated oracles
  - Security Notion: objective and capabilities



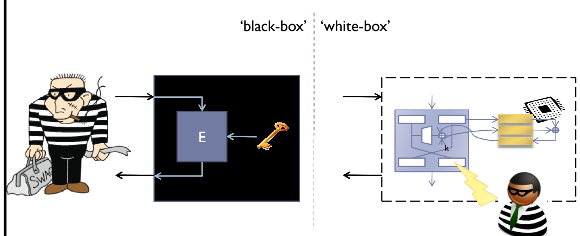
Example security notion: **KR-CPA**

- Key Recovery under Chosen Plaintext Attack



Our main research question

How can cryptographic primitives be implemented in software, such that they remain secure?



Our Contributions

- Practical implementations (Chapter 3)
  - Cryptanalysis of white-box DES implementations
  - Analysis of basic building blocks and invertibility issue
- Formal model (Chapter 4)
  - Formalizing white-box cryptography
  - Positive and negative results
  - Extensions towards probabilistic primitives
- Applications (Chapter 5)
  - Links with diverse related techniques
  - Development of practical solutions in software security

Overview

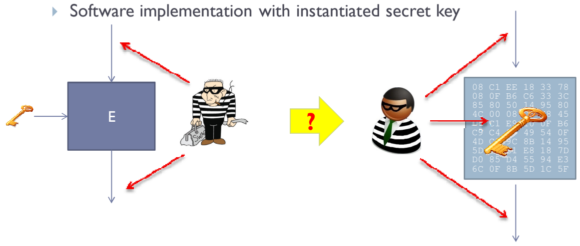
- Introduction
- White-box security assessment
  - White-box implementations (Chapter 3)
  - Formal model and (im)possibility result (Chapter 4)
- Applications and related research domains (Chapter 5)
- Conclusions and future work

Overview

- Introduction
- White-box security assessment
  - White-box implementations
  - Formal model and (im)possibility result
- Applications and related research domains
- Conclusions and future work

White-Box Implementations

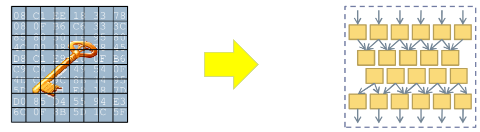
- The single line of defense is HOW to implement a cipher.
  - Software implementation with instantiated secret key



- Goal: Effort of analysis ≥ BB attack
- Ideal: Implement the cipher as one big lookup table

Obfuscation Strategy

- S. Chow, P. Eisen, H. Johnson, and P.C. van Oorschot, 2002 [42,43]
  Implement a *block cipher* as a network of randomized lookup tables

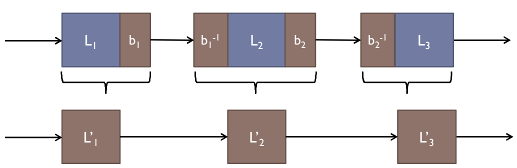


- Idea:
  - Spread key information on the entire network
  - Make every building block seemingly independent from the key.
- Objective: force an adversary to analyze the complete network in order to obtain secret key information → force to resort to black-box attacks.
- Techniques: partial evaluation, by-pass encoding, matrix decomposition, etc.

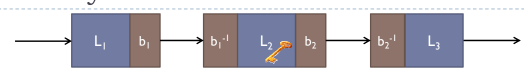
Internal encodings

- Consider the chain $L_3 \circ L_2 \circ L_1$
- L_2 contains key information
- Obfuscate L_2 with the bijections b_1, and b_2
- Encoded chain: $L_3' \circ L_2' \circ L_1'$

$$\begin{cases} L_1 & \rightarrow & L_1' = b_1 \circ L_1 \\ L_2 & \rightarrow & L_2' = b_2 \circ L_2 \circ b_1^{-1} \\ L_3 & \rightarrow & L_3' = L_3 \circ b_2^{-1} , \end{cases}$$



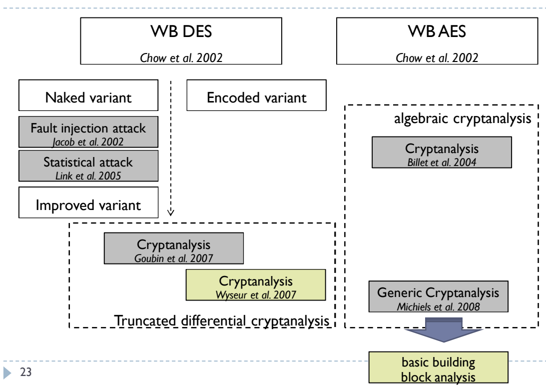
Security of encoded networks



- Local security
  - If $L_2 = f_k$ is bijective, then L'_2 is *locally secure*, because
    $$\forall k, \exists\ b_1, b_2 \text{ such that } L_2' = b_1^{-1} \circ f_k \circ b_2$$
  - This is infeasible to map to entire implementation (Lynn *et al.*, 2004 [118])
- Global Security?
  - Metrics
    - Diversity $k \Rightarrow \#L'$
    - Ambiguity $L' \Rightarrow \#k$
  - Scrutiny → Chapter 3
  - Prove → Chapter 4

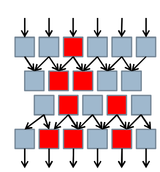
$$\begin{cases} L_1 & \rightarrow & L_1' = b_1 \circ L_1 \\ L_2 & \rightarrow & L_2' = b_2 \circ L_2 \circ b_1^{-1} \\ L_3 & \rightarrow & L_3' = L_3 \circ b_2^{-1} , \end{cases}$$

State of the art



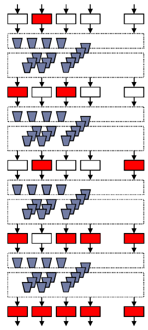
Differential cryptanalysis

- Introduce a difference (targeted fault) in the application
- Observe the fault propagation
- Learn.



- Deployed to analyze white-box implementations at the 'edges' of the implementation (first/last round)
- In this dissertation: a new strategy of truncated differential cryptanalysis on the internal rounds (hence independent from external protections)

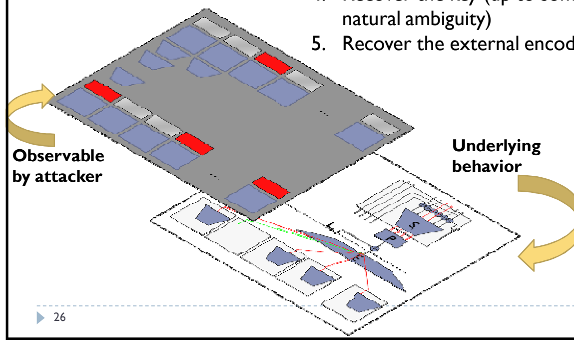
Cryptanalysis of White-Box DES Impl.



- Wyseur *et al.*, 2007 [191]
- Cryptanalysis on internal round structure, independent of external encodings
- Strategy:
  1. Distinguish round input differences that propagate *slow*
  2. Construct set of differences that correspond to flips of single bits at input of DES S-boxes
  3. …

Cryptanalysis of WBDES (2) (Wyseur et al., 2007 [191])

3. Compute inputs to the S-boxes
4. Recover the key (up to some natural ambiguity)
5. Recover the external encodings



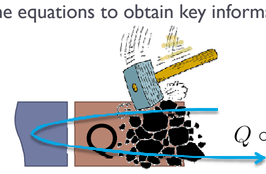
Algebraic Cryptanalysis

- Main strategy:
  - Remove the non-linear component of the internal encodings

Theorem 1 (O. Billet, H. Gilbert and C. Ech-Chatbi, 2004 [20]):

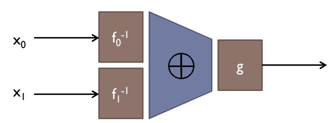
$$\boxed{\mathcal{S} = \{Q \circ \oplus_\beta \circ Q^{-1}\}_{\beta \in \mathrm{GF}(2^8)} \text{ yields } \tilde{Q} \text{, with } A = \tilde{Q} \circ Q \text{ affine}}$$

  - Construct algebraic equations
  - Solve the equations to obtain key information.

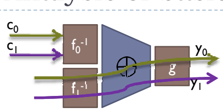


Algebraic cryptanalysis

- Demonstrated on white-box AES implementation
  (O. Billet, H. Gilbert and C. Ech-Chatbi, 2004 [20])
- Extended to 'SLT' ciphers (includes MDS-based ciphers)
  (W. Michiels, P. Gorissen and H. Hollmann, 2008 [135])
- … towards analysis of block cipher building blocks
  (our contribution)
  - Example: encoded addition operation



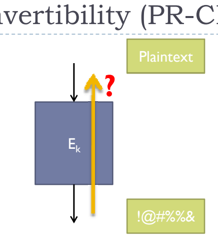
Analysis of basic building block



$$\begin{cases} y_0 := g \circ \bigoplus_{f_0^{-1}(c_0)} \circ f_1^{-1} \\ y_1 := g \circ \bigoplus_{f_0^{-1}(c_1)} \circ f_1^{-1} \end{cases}$$

- Hence: $y_1 \circ y_0^{-1} = g \circ \bigoplus_{f_0^{-1}(c_1) \oplus f_0^{-1}(c_0)} \circ g^{-1}$
- The family of functions $\{g \circ \oplus_c \circ g^{-1}\}_{c \in \mathrm{GF}(2^4)}$ yields information on the encoding g.
- The obtained information can be used as an alternative approach to cryptanalysis the DES and AES implementations.

Invertibility (PR-CPA)



- KR-CPA is often not satisfactory
- PR-CPA *(plaintext recovery under chosen plaintext attack)* is much more interesting in practice
- wbAES: 2^{32} – because lookup tables work on per-column basis
- wbDES: 2^{96} (>> 2^{56}, DES natural resistance)
  - Because of the use of parallel, encoded addition networks of 96 bits to 4 bits
  - But, XOR building block analysis defeats non-linearity of these networks

Conclusions chapter 3

- White-box implementations of DES and AES are insecure
  - Differential cryptanalysis
  - Algebraic cryptanalysis
- Attacks are specific to the cryptographic primitive, or a building block that is present.
  - Towards a block cipher with building blocks that is suitable to be implemented in software
  - Proposals are formulated in dissertation.
- Extensions towards non-invertibility and key update

Overview

- Introduction
- White-box security assessment
  - White-box implementations
  - Formal model and (im)possibility result
- Applications and related research domains
- Conclusions and future work

Formal approach to WBC

- Objectives
  - Formalize white-box cryptography
  - Capture the security of white-box solutions (beyond scrutiny)
  - What is feasible?
    - Negative results
    - Positive results
- Related
  - Theoretical models for Obfuscation

    Obfuscation – hide characteristics of a program P

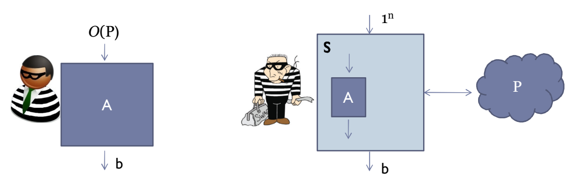
    (program code, internal data values, sensitive routines, etc.)

    O is an obfuscator, *O*(P) functionally equivalent obfuscated program.

Obfuscation – soundness

- Predicate-based definition (Barak *et al.*, 2001 [6])

$$\left|\Pr\left[A(\mathcal{O}(P))=\pi(P)\right]-\Pr\left[S_A^P(1^{|P|})=\pi(P)\right]\right|\leq \mathrm{neg}(|P|)$$

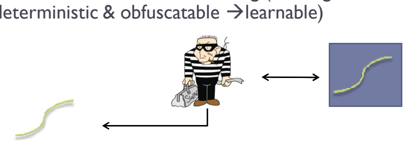


- Distinguisher-based definition

$$\left|\Pr\left[D(A(\mathcal{O}(P)))=1\right]-\Pr\left[D(S^P(1^{|P|}))=1\right]\right|\leq neg(|P|)$$

Models for Obfuscation

- Many models and results have been presented, but…
  - Predicate-based definition is too weak (meaningless)
  - Distinguisher-based definition is too strong (nothing interesting possible: deterministic & obfuscatable → learnable)
- Learnable



  - Learnable functions not of our interest
    - Cryptographic scheme's should be non-learnable.
- Also, obfuscation cannot capture cryptographic security requirements

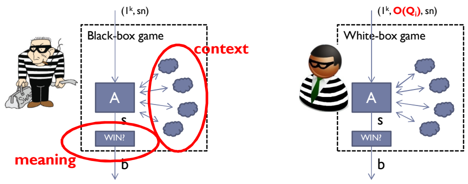
Our approach to capture WBC

- A new model, based on predicate-based notion for obfuscation, specific to WBC

  (Saxena and Wyseur, 2008 [165])
- We capture "meaning" with security notions
  - Attack goals
  - Attack capabilities (described as a game between a challenger and the adversary)

  "White-Box Property"

Our approach to capture WBC (2)



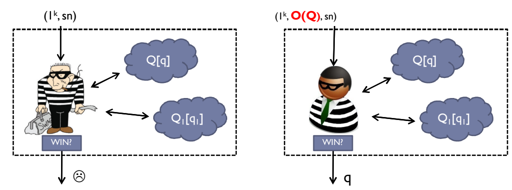
$$\begin{cases} \mathrm{AdvBB}^{sn}_A(k) = \Pr\left[r \xleftarrow{R} \{0,1\}^{p_{in}(k)} : \mathrm{GameBB}_A(1^k, sn, r) = 1\right] \\ \mathrm{AdvWB}^{sn}_{A,O,Q_i}(k) = \Pr\left[r \xleftarrow{R} \{0,1\}^{p_{in}(k)} : \mathrm{GameWB}_{A,O,Q_i}(1^k, sn, r) = 1\right] \end{cases}$$

- *O* is a secure obfuscator for Q_i, under the *sn* security notion, if $\left|\max_{A\in \mathrm{PPT}} \mathrm{AdvWB}^{sn}_{A,O,Q}(k) - \max_{A\in \mathrm{PPT}} \mathrm{AdvBB}^{sn}_A(k)\right| \le neg(|k|)$

37

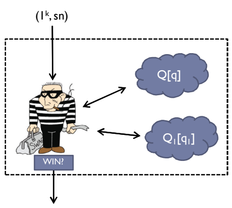
Negative results (Saxena and Wyseur, 2008 [165])

- For any non learnable family Q, there exist a non-obfuscatable security notion (this is stronger than Barak *et al.*, 2001)



38

Proof of impossibility result

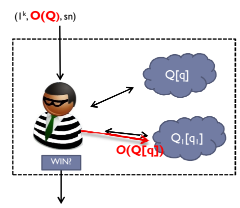


- $Q_1[q_1]$ (input Y) {
  If (Y(a) = Q[q](a)) then
  output x
  else output 0 }
- Q is non-learnable
  $$\begin{cases} q \xleftarrow{R} \{0,1\}^k \\ x \xleftarrow{R} \{0,1\}^k \\ a \xleftarrow{R} \{0,1\}^{\mathbf{P_Q(k)}} \end{cases}$$
- Win: if (s=x) and 'not more than one query to Q_1'
- BB adversary – how to find x?
  - Guess x – prob: 2^{-k}
  - Guess a – prob: $2^{-P(k)}$
  - Guess q – prob: 2^{-k}
  - Luck

Black-box advantage: $\forall A \in \mathrm{PPT} : 0 \le \mathrm{AdvBB}^{guess\text{-}x}_A(k) < \alpha(k)$

39

Proof of impossibility result (2)



- $Q_1[q_1]$ (input Y) {
  If (Y(a) = Q[q](a)) then
  output x
  else output 0 }
- Q is non-learnable
  $$\begin{cases} q \xleftarrow{R} \{0,1\}^k \\ x \xleftarrow{R} \{0,1\}^k \\ a \xleftarrow{R} \{0,1\}^{\mathbf{P_Q(k)}} \end{cases}$$
- Win: if (s=x) and 'not more than one query to Q_1'
- WB adversary – how to find x?
  - Use the code *O*(Q[q]) as Y

White-box advantage: $\exists A \in \mathrm{PPT} : 1 \ge \mathrm{AdvWB}^{guess\text{-}x}_{A,O,Q}(k) \ge 1 - \beta(k)$

40

Proof of impossibility result (3)

- Black-box adversary:
  $$\forall A \in \mathrm{PPT} : 0 \le \mathrm{AdvBB}^{guess\text{-}x}_A(k) < \alpha(k)$$
- White-box adversary:
  $$\exists A \in \mathrm{PPT} : 1 \ge \mathrm{AdvWB}^{guess\text{-}x}_{A,O,Q}(k) \ge 1 - \beta(k)$$
- White-box property: *O* is secure for *Q* under sn, if:
  $$\left|\max_{A\in \mathrm{PPT}} \mathrm{AdvWB}^{sn}_{A,O,Q}(k) - \max_{A\in \mathrm{PPT}} \mathrm{AdvBB}^{sn}_A(k)\right| \le neg(|k|)$$
- But:
  $$\left|\max_{A\in PPT} AdvWB^{sn}_{A,O,Q}(k) - \max_{A\in PPT} AdvBB^{sn}_A(k)\right| > 1 - \alpha(k) - \beta(k)$$

$\square$

41

Positive result (Saxena and Wyseur, 2008 [165])

- There exists an obfuscator *O* that turns a IND-CPA secure, symmetric encryption scheme into an IND-CPA secure asymmetric encryption scheme
- Based on the bi-linear Diffie-Hellman assumption

- Remark: positive result is based on a cipher that consists of asymmetric building blocks (pairings). We started with white-box crypto for symmetric encryption schemes (DES, AES).

42

Overview

- Introduction
- White-box security assessment
  - White-box implementations
  - Formal model and (im)possibility result
- Applications and related research domains
- Conclusions and future work

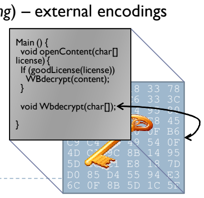
Applications

- Application domains
  - New and improved cryptographic primitives
    - Asymmetric cryptography
    - (Programmable) random oracle model
  - Enforce (with) hardware
    - Improve side-channel protection techniques
  - Computing in the encrypted domain
    - Homomorphic encryption
    - Secure function evaluation (Yao's garbled circuits)
  - Software protection
    - Software tamper resistance
    - Software diversity
    - Trustworthy execution (TC, remote entrusting, WBRPE)
- Case study
  - Digital Rights Management
    - Traitor tracing

Related techniques

Software security

- White-box cryptography is only a small piece in the puzzle.
  - 128-bit AES key → 770 Kbytes key (the white-box AES implementation lookup tables)
  - Now we got a larger key… so what?
  - Result is more flexible
    - Fix key into the application (prevent *code lifting*) – external encodings
    - A leverage for other software protection techniques
      - Traitor tracing
      - Obfuscation
      - Software Tamper Resistance
      - …



Overview

- Introduction
- White-box security assessment
  - White-box implementations (Chapter 3)
  - Formal model and (im)possibility result (Chapter 4)
- Applications and related research domains (Chapter 5)
- Conclusions and future work

Conclusions and Future Research

- White-Box Implementations
  - State of the art implements shown to be insecure
  - Analysis of basic building blocks (lead to alternative attacks and defeat of PR-CPA security)
  - Future work: towards new block ciphers and design principles
- Theoretic model for White-Box Cryptography
  - A formal model has been introduced – context captured by security notions
  - Positive and negative results have been presented
  - A provably IND-CPA secure white-box implementation
  - Future work: prove other constructions – extensions towards probabilistic functions
- Applications
  - Use of WBC in practice, and relation with other research fields
  - Future work: investigate new directions, inspired by other fields

Publications

- Papers
  - A. Saxena, B. Wyseur, "On White-Box Cryptography and Obfuscation", IACR ePrint 2008/273, 2008 – to be submitted to *22nd IEEE Computer Security Foundations Symposium (CSF 2009).*
  - D. Schellekens, B. Wyseur, B. Preneel, "Remote Attestation on Legacy Operating Systems with Trusted Platform Modules", In *1st International Workshop on Run-Time Enforcement of Mobile and Distributed Systems (REM 2007) – Science of Computer Programming*, 2008
  - B. Wyseur, W. Michiels, P. Gorissen, B. Preneel, "Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings", In *Proceedings of 14th International Workshop on Selected Areas in Cryptology (SAC 2007).*
  - K. Wouters, B. Wyseur, B. Preneel, "Security Model for a Shared Multimedia Archive", In *Proceedings of the Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution(AXMEDIS 2007).*
  - K. Wouters, B. Wyseur, B. Preneel, "Lexical Natural Language Steganography Systems with Human Interaction", In *Proceedings of the 6th European Conference on International Warfare and Security* (ECIW *2007).*
  - B. Wyseur, K. Wouters, M. Deng, T. Herlea, B. Preneel, "On the Design of a Secure Multimedia Archive", In *1st Benelux Worskhop on Information and System Security (WISSec 2006).*
  - B. Wyseur, B. Preneel, "Condensed White-Box Implementations", In *Proceedings of 26th Symposium on Information Theory in the Benelux (BSIT 2005).*
- Reports
  - S. Faust, B. Wyseur, G. Neven, "PIN based digital lockers", 2008
  - B. Wyseur, M. Deng, T. Herlea, "A Survey on Homomorphic Encryption Schemes", 2007
  - J. Cappaert, B. Wyseur, B. Preneel, "Software Security Techniques", 2004

Q&A

- Thank you.