Tancrède Lepoint (S.C.C.I. 2011)

10-th birthday S.C.C.I, September 12, 2011

technicolor

Presentation

- **Scholarship**
  - Master 1 Pure Mathematics (2009 – 2010)
  - Master 2 **S.C.C.I** (2010 – 2011)

- Internship at **Technicolor**

Internship Subject

How to design a white-box implementation for an asymmetric cryptographic primitive?

technicolor

Presentation

- **Scholarship**
  - Master 1 Pure Mathematics (2009 – 2010)
  - Master 2 **S.C.C.I** (2010 – 2011)

- Internship at **Technicolor**

Internship Subject

How to design a white-box implementation for an asymmetric cryptographic primitive?

technicolor

White-Box Cryptology Motivations

- Malicious software on the user machine: search entropy

  (Shamir and Van Someren, 1999)

  Keys need to be chosen at random (high entropy); code contains structure (low entropy)

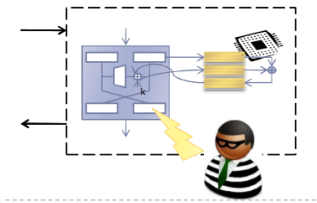
- DRM: main application is to secure distribution of 'valuable' content. Decryption routine:
  - Hardware (*e.g.*, set-top box)
  - Software (*e.g.*, iTunes)

  Platforms cannot be trusted

technicolor

White-Box Model

- Powerful adversary: possible to view and alter at will the algorithm and the dynamic execution environment
- Goal: protect the key on an unsecure environment
- Worse possible model



Security

A implementation secured against WB attacks is secure against BB attacks and existant and *any future* GB attacks

technicolor

Symmetric primitives (1)

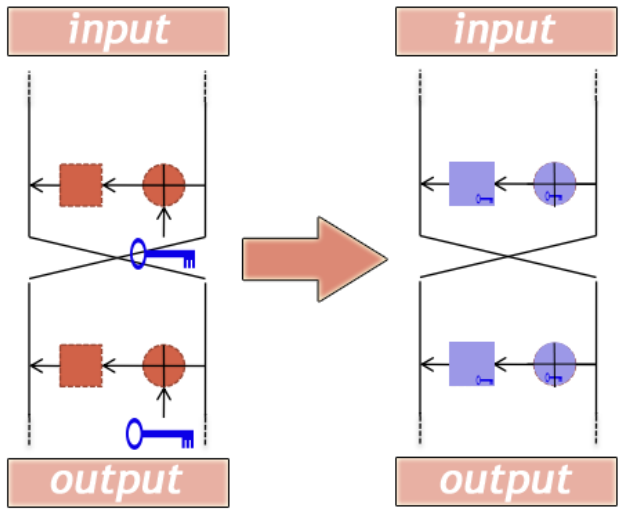
- State-of-the-art: symmetric primitives (AES and DES, Chow *et al.* in 2002)
- Technique for hiding secret keys in software implementation

Operation

Rewrite a key-instantiated version of a block cipher

Symmetric primitives (1)

- State-of-the-art: symmetric primitives (AES and DES, Chow *et al.* in 2002)
- Technique for hiding secret keys in software implementation

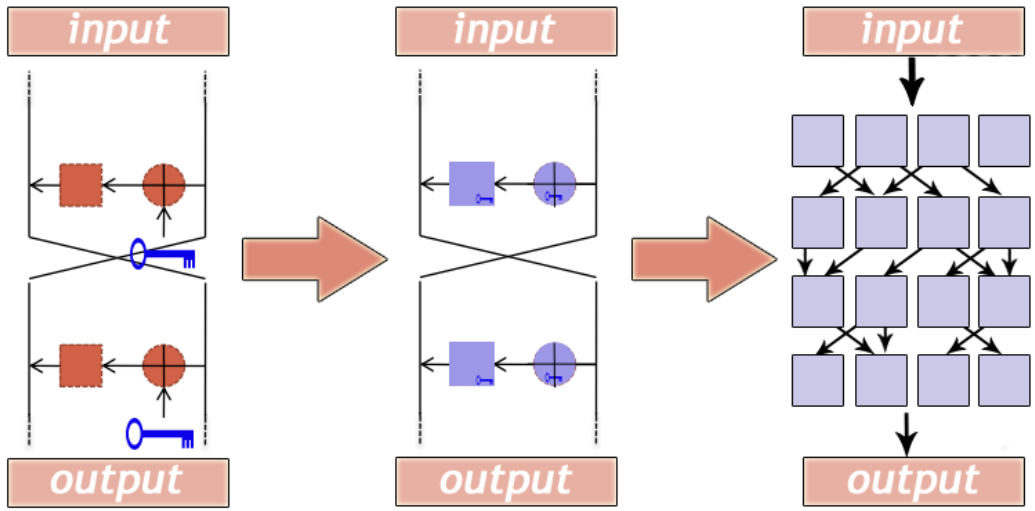


Operation

Rewrite a key-instantiated version of a block cipher

Symmetric primitives (1)

- State-of-the-art: symmetric primitives (AES and DES, Chow *et al.* in 2002)
- Technique for hiding secret keys in software implementation



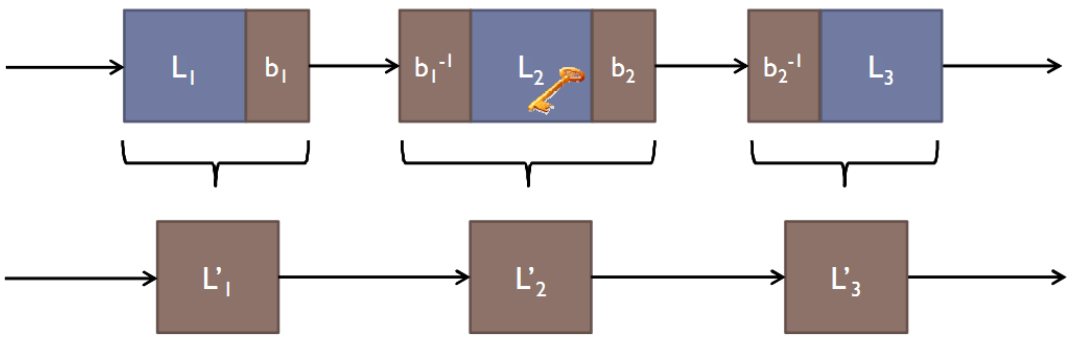
Operation

Transform into a randomized network of key-instantiated look-up tables

Symmetric primitives (2)

Operation

Randomization and delinearization



Patent of Irdeto

- White-Box implementation of RSA?

Main idea

Add a multiple of $\phi(N)$ to private key d:

$$d^* = d + k\phi(N), \qquad k > 0$$

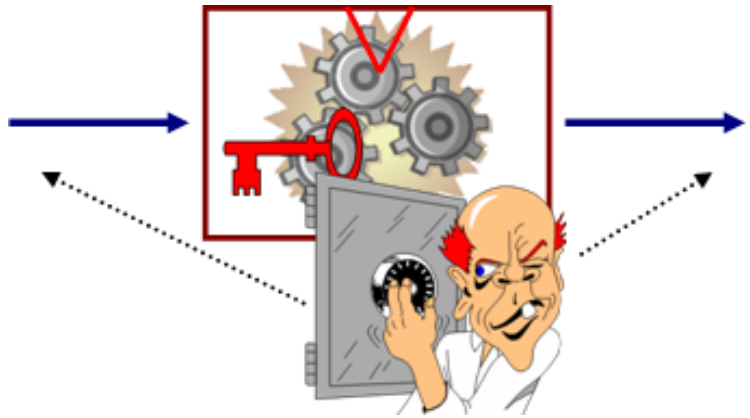
Remarks

- Contribution: Broken with Miller's algorithm in WB context
- Not a new idea: used in smart-card

technicolor

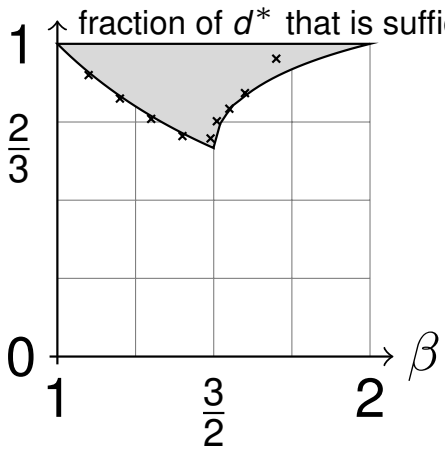
In grey-box context?

- Partial Key Exposure attacks when $d > N$

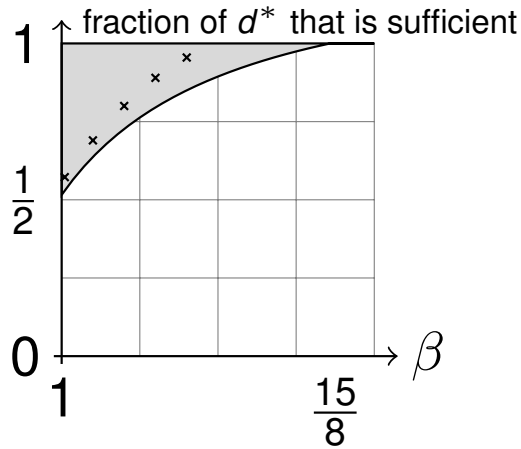


Contributions

Attacks when MSBs or LSBs are known



MSB



LSB

technicolor

Ideas for asymmetric primitives

- Tabularizing the exponentiation (RSA, El-Gamal, . . .)
  - Use of the RNS
  - combined with Montgomery Modular Multiplication
- Tabularizing the polynomial modular multiplication
  - Spectral arithmetic

Problem

At one point: LUTs not possible, and cannot be obfuscated easily

- But reduction of WB implementation of RSA to WB implementation of basis extension

Conclusion

Contributions

- White-box implementation (of RSA) reduced to implement basis extension in a WB fashion
- Attack on a patent of Irdeto (with Miller's algorithm)
- Theorems on MSBs and LSBs attacks
- Design of a software decoder to allow traitor tracing

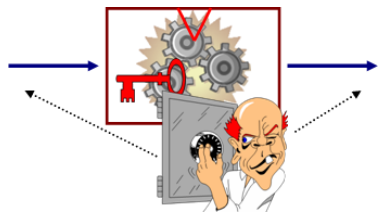
Keywords

White-box, grey-box, lattices, traitor tracing, RNS, Montgomery multiplication, spectral arithmetic

technicolor

Produced Papers

- *Traitor Tracing Schemes for Protected Software Implementations* (with Marc Joye), **to appear** in *11th ACM Workshop on Digital Rights Management (ACM-DRM 2011)*, Chicago, USA, October 21, 2011;
- Patent application #11305865.5, *TRAITOR TRACING FOR SOFTWARE-IMPLEMENTED DECRYPTION ALGORITHMS* (with Marc Joye), **filed** on July 6, 2011;
- *Partial Key Exposure on RSA with Private Exponents Larger than N* (with Marc Joye), **submitted for publication**.



Comments/Questions?

Thank you!