



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles
Random
oracles
The Delphic
Oracle

The main
result

Conclusion

Bibliography

Perfect Localized Security of the Fourtytwofish Cipher in the Delphic Oracle Model

La spatialisation de Poisson
de Pharse à Trappes

David A. Madore
TELECOM ParisTech
david.madore@enst.fr
<http://perso.enst.fr/~madore/>



1 Background on the fourtytwofish cipher

- History
- Localized security
- Goals of fourtytwofish
- Design

2 Oracles and security

- Oracles
- Random oracles
- The Delphic Oracle

3 The main result

4 Conclusion

5 Bibliography



Belongs to a **long line of ciphers** by **respected cryptographers**:

- Blowfish (B. Schneier, 1993)
- Twofish (B. Schneier & al, 1998)
- Threefish (H. Sonnenregner, 1999) — broken 1999
- Fourfish (H. Sonnenregner, 1999) — broken 1999
- Fivefish (H. Sonnenregner, 1999) — broken 2000
- Sixfish (H. Sonnenregner, 2000) — broken 2000
- ...
- Fourtyfish (H. Sonnenregner, 2007) — broken 2008
- Fourtyonefish (H. Sonnenregner, 2008) — broken 2008
- Fourtytwofish (H. Sonnenregner, 2008)

Note: some (but not all) were broken.

Fortytwofish

David A.
Madore

Outline

Fortytwofish
background

History

Localized
security

Goals

Design

Oracles and
security

Oracles

Random
oracles

The Delphic
Oracle

The main
result

Conclusion

Bibliography

What is ordinary security?

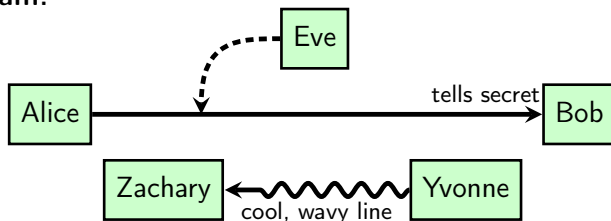


Ordinary security

Alice uses the cipher to **tell Bob a secret**

The attacker Eve (“eavesdropper”) **cannot guess the secret** without knowing the encryption key

Diagram:



Note: Yvonne and Zachary have fun with TikZ while Alice tells Bob her meaningless secret.

Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History

Localized
security

Goals

Design

Oracles and
security

Oracles

Random
oracles

The Delphic
Oracle

The main
result

Conclusion

Bibliography

What is *localized* security?



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History

Localized
security

Goals

Design

Oracles and
security

Oracles

Random
oracles

The Delphic
Oracle

The main
result

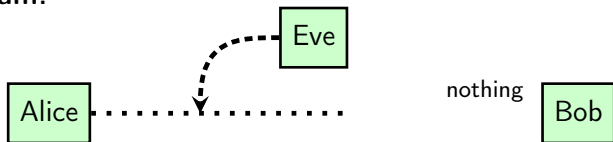
Conclusion

Bibliography

Localized security

Now Alice **does not tell Bob** the secret at all

Diagram:



What is *localized* security?



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History

Localized
security

Goals
Design

Oracles and
security

Oracles
Random
oracles
The Delphic
Oracle

The main
result

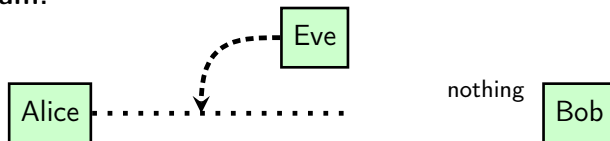
Conclusion

Bibliography

Localized security

Now Alice **does not tell Bob** the secret at all

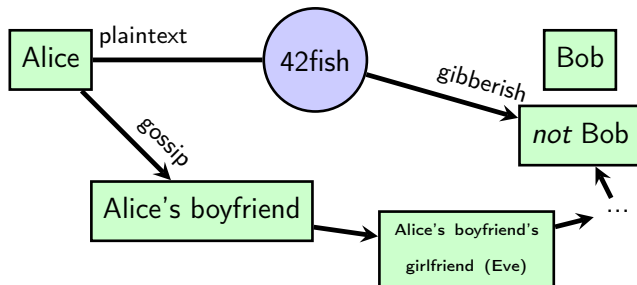
Diagram:



Much more **difficult**: ever try to keep a secret for yourself?

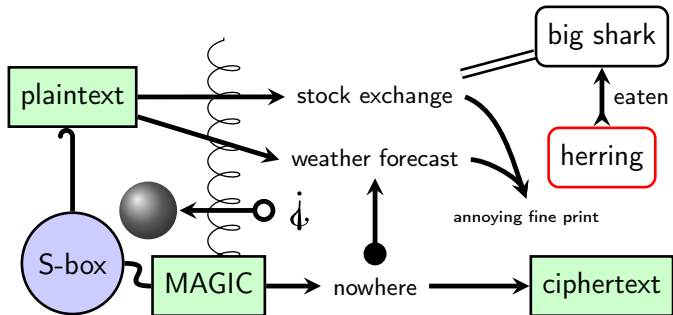


Another cool TikZ picture:



Design principles

- Simple and elegant design
- No unexplained pieces
- Peer-reviewed on Slashdot.org

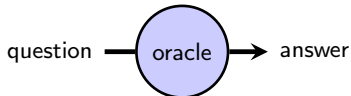




ORACLE[®]

How an Oracle works

- Question goes in
- Sacrifice made to gods (or higher powers: computers...)
- Divinely inspired answer comes out



Example: 易經 (made in China)

Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles
Random
oracles
The Delphic
Oracle

The main
result

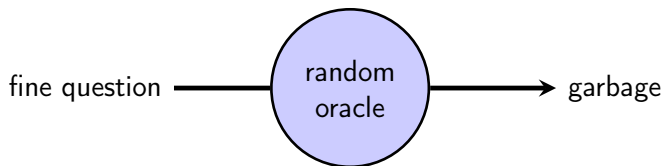
Conclusion

Bibliography

What is a random oracle?



Cheap plastic imitation of a real oracle, often used in cryptography:



Fortytwofish

David A.
Madore

Outline

Fortytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles

Random
oracles

The Delphic
Oracle

The main
result

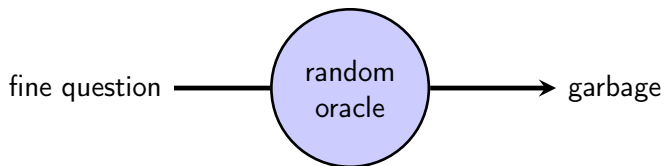
Conclusion

Bibliography

What is a random oracle?



Cheap plastic imitation of a real oracle, often used in cryptography:



Example:

— Tell me, O Mighty Oracle, tell me the answer to my question: how can I make out with Brad Pitt¹?

¹Replace with Angelina Jolie according to your tastes.

Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles

Random
oracles

The Delphic
Oracle

The main
result

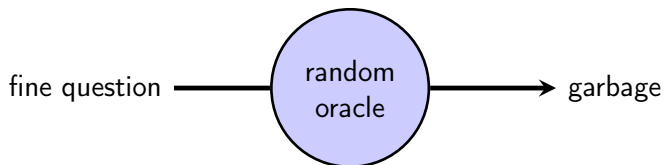
Conclusion

Bibliography

What is a random oracle?



Cheap plastic imitation of a real oracle, often used in cryptography:



Example:

— Tell me, O Mighty Oracle, tell me the answer to my question: how can I make out with Brad Pitt¹?

— 5d9ba10c8d2d8d6b1b597f11d55cc435237669ae

Not very useful!

¹Replace with Angelina Jolie according to your tastes.

Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles

Random
oracles

The Delphic
Oracle

The main
result

Conclusion

Bibliography



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History

Localized
security

Goals

Design

Oracles and
security

Oracles

Random
oracles

The Delphic
Oracle

The main
result

Conclusion

Bibliography

Idea: instead of these useless random oracles, introduce the **Delphic Oracle** in cryptographic proofs.



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles
Random
oracles

The Delphic
Oracle

The main
result

Conclusion

Bibliography

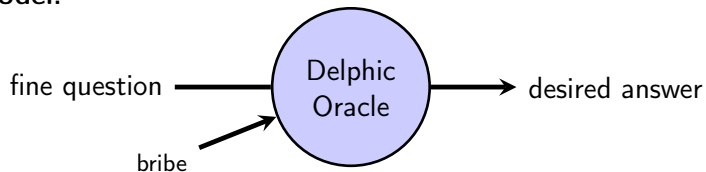
Idea: instead of these useless random oracles, introduce the **Delphic Oracle** in cryptographic proofs.

The Delphic Oracle

- Established in Delphi, Greece (circa 8th century BCE)
- Presided by priestess of Apollo
- Respectable reputation
- Foretold Alexander's conquests, Nero's death, Hadrian's rise as Emperor, etc.



Model:



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles
Random
oracles

The Delphic
Oracle

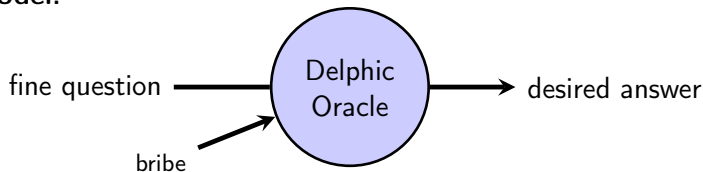
The main
result

Conclusion

Bibliography



Model:

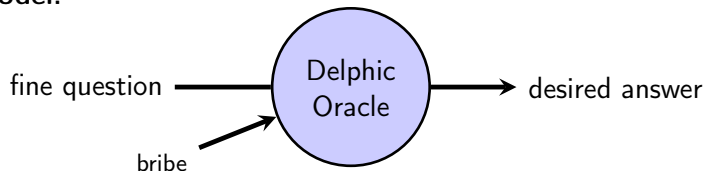


Example:

— Tell me, O Mighty Oracle, tell me the answer to my question: is my cunningly devised cipher unbreakable?



Model:

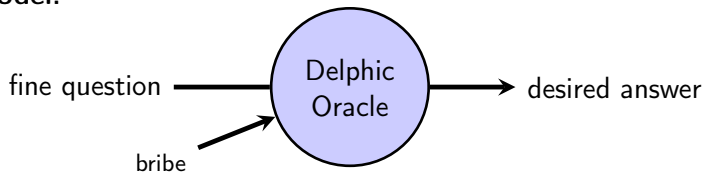


Example:

— Tell me, O Mighty Oracle, tell me the answer to my question: is my cunningly devised cipher unbreakable?

— Of course it is, Sir. Now, do you wish to buy a stucco bust of Socrates for only 9.99€?

Model:



Example:

— Tell me, O Mighty Oracle, tell me the answer to my question: is my cunningly devised cipher unbreakable?

— Of course it is, Sir. Now, do you wish to buy a stucco bust of Socrates for only 9.99€?

Much more useful! (...except for the bust of Socrates, which is rather tacky)



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History

Localized
security

Goals

Design

Oracles and
security

Oracles

Random
oracles

The Delphic
Oracle

The main
result

Conclusion

Bibliography

Theorem

*Fourtytwofish achieves **perfect localized security** in the Delphic Oracle model.*



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles
Random
oracles
The Delphic
Oracle

The main
result

Conclusion

Bibliography

Theorem

*Fourtytwofish achieves **perfect localized security** in the Delphic Oracle model.*

Some techniques used in proof:

- Long abstruse results from algebraic geometry.
- Large body of numerical evidence.
- Vigorous handwaving.
- Personal communication / divine inspiration.
- Zero-content proof techniques.

The details are left as an exercise.



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles
Random
oracles
The Delphic
Oracle

The main
result

Conclusion

Bibliography

Assume

- X is a proper locally pseudo-factorial quasi-Gorenstein universally catenary almost everywhere noetherian semi-effective excellent log-scheme with at most \mathbb{Q} -divisorial and q -log-canonical singularities,
- $Y \xrightarrow{f} X$ is flat, crepant and smooth in codimension ≤ 2 with Y Cohen-Macaulay,
- $\ker[H^p(Y, f^*(\Omega_{X/Z}^q)^{\otimes n}) \rightarrow H^p(Y, f^*(\Omega_{X/Z}^q)^{\otimes n})] = 0$ for some n (for all p , for all q , for some $X \rightarrow Z$);



Assume

- X is a proper locally pseudo-factorial quasi-Gorenstein universally catenary almost everywhere noetherian semi-effective excellent log-scheme with at most \mathbb{Q} -divisorial and q -log-canonical singularities,
- $Y \xrightarrow{f} X$ is flat, crepant and smooth in codimension ≤ 2 with Y Cohen-Macaulay,
- $\ker[H^p(Y, f^*(\Omega_{X/Z}^q \otimes^n)) \rightarrow H^p(Y, f^*(\Omega_{X/Z}^q) \otimes^n)] = 0$ for some n (for all p , for all q , for some $X \rightarrow Z$);

then

- the obvious conclusion follows.

Note in terminology: $2 := 1 + 1$.



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History

Localized
security

Goals

Design

Oracles and
security

Oracles

Random
oracles

The Delphic
Oracle

The main
result

Conclusion

Bibliography

Expected applications:

- Patents
- Lots of money



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles
Random
oracles
The Delphic
Oracle

The main
result

Conclusion

Bibliography

Expected applications:


- Patents
- Lots of money

Applications so far:

- Talks at prestigious conferences
- Busts of Socrates, Pericles, etc. (made of stucco)



[refneeded] Anonymous (author unknown),
Reference needed, (cited in [Wikipedia]).

 Prestigious author,
Prestigious title having nothing to do with Fortytwofish,
Presitigious journal.

 God,
The Bible.

▶ God,
personal communication.

[Wikipedia] J. Wales & al.,
Wikipedia,
published online.

Fortytwofish

David A.
Madore

Outline

Fortytwofish
background

History

Localized
security

Goals

Design

Oracles and
security

Oracles

Random
oracles

The Delphic
Oracle

The main
result

Conclusion

Bibliography



Fourtytwofish

David A.
Madore

Outline

Fourtytwofish
background

History
Localized
security
Goals
Design

Oracles and
security

Oracles
Random
oracles
The Delphic
Oracle

The main
result

Conclusion

Bibliography

So long, and thanks for all the fish!

(Any questions?)