Constructive Cryptography by U Maurer

Review by Ajay Sharma

October 2014
Table of Contents

1. Most Interesting points made
2. Most important message
3. Comparison to previous research
4. Improvement in Proof style and readability
Table of Contents

1. Most Interesting points made
2. Most important message
3. Comparison to previous research
4. Improvement in Proof style and readability
A new paradigm for defining the security of cryptographic schemes such as

- Symmetric encryption
Most interesting points made

A new paradigm for defining the security of cryptographic schemes such as
- Symmetric encryption
- Message authentication codes
Most interesting points made

A new paradigm for defining the security of cryptographic schemes such as
- Symmetric encryption
- Message authentication codes
- Public-key encryption
Most interesting points made

A new paradigm for defining the security of cryptographic schemes such as
- Symmetric encryption
- Message authentication codes
- Public-key encryption
- Key-agreement protocols
A new paradigm for defining the security of cryptographic schemes such as

- Symmetric encryption
- Message authentication codes
- Public-key encryption
- Key-agreement protocols
- Digital signature schemes
Most interesting points made

- Constructive cryptography is a new paradigm in which the security definition of cryptographic schemes is radically different.
Constructive cryptography is a new paradigm in which the security definition of cryptographic schemes is radically different.

Security problems of the One-Time Pad
In this paper
In this paper what is the
In this paper, what is the single most important message?
Table of Contents

1. Most Interesting points made

2. Most important message

3. Comparison to previous research

4. Improvement in Proof style and readability
One can separate the understanding of what cryptography achieves from the technical security definitions and proofs, which is useful for didactic purposes and protocol design.
Table of Contents

1. Most Interesting points made
2. Most important message
3. Comparison to previous research
4. Improvement in Proof style and readability
The term *construct*, which is defined by the use of a simulator, is composable in the sense that a protocol obtained by the composition of several secure constructive steps is *itself secure*. This is in contrast to both the *traditional, game-based security* definitions for cryptographic schemes and the *attack-based security* definitions used in formal-methods based security research, which are generally not composable.
Table of Contents

1. Most Interesting points made
2. Most important message
3. Comparison to previous research
4. Improvement in Proof style and readability
Many points in any single proof have a citation to some other paper. This is too clumsy for a reader to go to a new paper everytime they try to read a proof.
Improvement points

- Many points in any single proof have a citation to some other paper. This is too clumsy for a reader to go to a new paper everytime they try to read a proof.
- Less diagrams used to explain the traditional security methods and their contrast with the new method the author introduces.