Computer-Aided Search Heuristic for Blind Revocable Identity Based Encryption Schemes

Tom Berson, Nigel Smart, Raphael C.-W. Phan,
Orr Dunkelman, Dan Page

On Behalf of the Best Open Access Journal in its Field
whose legendary Impact Factor of 0 is unmatched.
Now with even shorter review process!

16 August, 2011

Computer-Aided Searches in Cryptography

- Yesterday we've heard how computer-aided searches succeeded in beating cryptographers in finding new attacks.
- However, this is not a new fact...

Computer-Aided Searches in Cryptography

- Yesterday we've heard how computer-aided searches succeeded in beating cryptographers in finding new attacks.
- However, this is not a new fact...
- Chaum and Evertse used computer-aided search in their seminal paper from CRYPTO'85.

Computer-Aided Searches in Cryptography

- Yesterday we've heard how computer-aided searches succeeded in beating cryptographers in finding new attacks.
- However, this is not a new fact...
- Chaum and Evertse used computer-aided search in their seminal paper from CRYPTO'85.
- Some claim that automatic solvers, such as SAT solvers or Gröbner base solvers are just a heuristic automated solvers.

Revocable Identity Based Encryption Schemes

- Introduced by Shamir in his CRYPTO 1984 paper, IBS and IBE became fundamental concepts in cryptography.
- Since the actual implementation of IBE by Boneh and Franklin in CRYPTO 2001, IBE became a very hot research topic.

Revocable Identity Based Encryption Schemes

- Introduced by Shamir in his CRYPTO 1984 paper, IBS and IBE became fundamental concepts in cryptography.
- Since the actual implementation of IBE by Boneh and Franklin in CRYPTO 2001, IBE became a very hot research topic.
- Various extensions to the basic IBE concept were introduced since:
  1. Hierarchal IBE (HIBE),
  2. Blind IBE (BIBE),
  3. Fuzzy IBE (FIBE),
  4. Wildcard IBE (WIBE),

Revocable Identity Based Encryption Schemes

- Introduced by Shamir in his CRYPTO 1984 paper, IBS and IBE became fundamental concepts in cryptography.
- Since the actual implementation of IBE by Boneh and Franklin in CRYPTO 2001, IBE became a very hot research topic.
- Various extensions to the basic IBE concept were introduced since:
  1. Hierarchal IBE (HIBE),
  2. Blind IBE (BIBE),
  3. Fuzzy IBE (FIBE),
  4. Wildcard IBE (WIBE),
- However, up until now, no primitive dealt with the problem of revoking an issued key in IBE schemes.

Uses of Revocable Identity Based Encryption Schemes

- When a secret key is exposed.

Uses of Revocable Identity Based Encryption Schemes

- When a secret key is exposed.
- When an employee leaves his work.

Uses of Revocable Identity Based Encryption Schemes

- When a secret key is exposed.
- When an employee leaves his work.
- When your identity is stolen (AKA identity theft).

Uses of Revocable Identity Based Encryption Schemes

- When a secret key is exposed.
- When an employee leaves his work.
- When your identity is stolen (AKA identity theft).
- When one changes his identity (e.g., split personality, a spy going under cover).

Uses of Revocable Identity Based Encryption Schemes

- When a secret key is exposed.
- When an employee leaves his work.
- When your identity is stolen (AKA identity theft).
- When one changes his identity (e.g., split personality, a spy going under cover).
- When one loses his identity (e.g., joins a cult, get brainwashed, bitten by a zombie).

Blind Revocable Identity Based Encryption Schemes

- We ran a computer-aided search on google, trying to find other uses for RIBE.

Blind Revocable Identity Based Encryption Schemes

- We ran a computer-aided search on google, trying to find other uses for RIBE.
- We found out that in several cases, e.g., a spy going undercover, we do not want that the center issuing the new identity will be able to know the new identity of the spy.

Blind Revocable Identity Based Encryption Schemes

- We ran a computer-aided search on google, trying to find other uses for RIBE.
- We found out that in several cases, e.g., a spy going undercover, we do not want that the center issuing the new identity will be able to know the new identity of the spy.
- Hence, we also introduce the concept of **Blind Revocable Identity Based Encryption Schemes**

Blind Revocable Identity Based Encryption Schemes

- We ran a computer-aided search on google, trying to find other uses for RIBE.
- We found out that in several cases, e.g., a spy going undercover, we do not want that the center issuing the new identity will be able to know the new identity of the spy.
- Hence, we also introduce the concept of **Blind Revocable Identity Based Encryption Schemes** (BRIBES).

Uses of CASH-BRIBES

- Very useful in several countries where the police and officials are not honest.

Uses of CASH-BRIBES

- Very useful in several countries where the police and officials are not honest.
- Frowned upon by several countries (such as the US), as part of their continuous fight against disseminating new cryptographic techniques.

Uses of CASH-BRIBES

- Very useful in several countries where the police and officials are not honest.
- Frowned upon by several countries (such as the US), as part of their continuous fight against disseminating new cryptographic techniques.
- Extremely useful when trying to have your paper published in the

Uses of CASH-BRIBES

- Very useful in several countries where the police and officials are not honest.
- Frowned upon by several countries (such as the US), as part of their continuous fight against disseminating new cryptographic techniques.
- Extremely useful when trying to have your paper published in the

Journal of Cryptology

Uses of CASH-BRIBES

- Very useful in several countries where the police and officials are not honest.
- Frowned upon by several countries (such as the US), as part of their continuous fight against disseminating new cryptographic techniques.
- Extremely useful when trying to have your paper published in the

Journal of Craptology

Journal of Craptology

- The journal of recreational cryptology.
- Started in 1998 (by our founding fathers, Lars, Keith, and Vincent).
- Revived in 2005 (by the current board).
- Latest volume — February 2010.
- Waiting for another paper to publish the new volume.

Call For Paper

Contributions must adhere to the strict criteria:

- Craptologic research
- Funny and amusing
- Controversial
- Non-offending (unless...)

New Directions in Craptology

- Wikileakage Resilient Cryptology.

New Directions in Craptology

- Wikileakage Resilient Cryptology.
- Fault attacks on tectonic boards.

New Directions in Craptology

- Wikileakage Resilient Cryptology.
- Fault attacks on tectonic boards.
- Random pseudo-numbers generators.

New Directions in Craptology

- Wikileakage Resilient Cryptology.
- Fault attacks on tectonic boards.
- Random pseudo-numbers generators.
- ...

Summary

Enjoy the short backlog and lack of page limit!

Past issues, more information, and lot's of crap(tology):

`http://www.anagram.com/~jcrap`