SaUCy

ANONYMOUS AUTHOR(S)

Text of abstract ....

Additional Key Words and Phrases: keyword1, keyword2, keyword3

1 INTRODUCTION

UC paper [Canetti 2001]. TODO: *Lots!*

2 OVERVIEW

3 ILC

4 METATHEORY

5 IMPLEMENTATION

6 EXPERIMENTS

Impossibility of UC commitments using standard assumptions [Canetti and Fischlin 2001].

Functionality $\mathcal{F}_{\text{COM}}$

$\mathcal{F}_{\text{COM}}$ proceeds as follows, running with parties $P_1, \ldots, P_n$ and an adversary S.

(1) Upon receiving a value $(\text{Commit}, sid, P_i, P_j, b)$ from P_i, where $b \in \{0, 1\}$, record the value b and send the message $(\text{Receipt}, sid, P_i, P_j)$ to P_j and S. Ignore any subsequent Commit messages.

(2) Upon receiving a value $(\text{Open}, sid, P_i, P_j)$ from P_i, proceed as follows: If some value b was previously recorded, then send the message $(\text{Open}, sid, P_i, P_j, b)$ to P_j and S and halt. Otherwise halt.

```
let F_com = lam S .
  let ('Commit, sid, P_i, P_j, b) = rd ?p2f in
    req mem b {0,1} in
    wr (('Receipt, sid, P_i, P_j), {P_j, S}) → ?f2p ;
    let ('Open, sid, P_i, P_j) = rd ?p2f in
    wr (('Open, sid, P_i, P_j, b), {P_j, S}) → ?f2p
in
  nu f2p, p2f .
    | ▹ (F_com S)
```

7 RELATED WORK

EasyCrypt [Barthe et al. 2011], CertiCrypt [Barthe et al. 2009], CryptoVerif [Blanchet 2007], ProVerif [Blanchet 2005], RF* [Barthe et al. 2014], Cryptol [Lewis and Martin 2003]

2018. 2475-1421/2018/1-ART1 $15.00
https://doi.org/

8 CONCLUSION

REFERENCES

Gilles Barthe, Cédric Fournet, Benjamin Grégoire, Pierre-Yves Strub, Nikhil Swamy, and Santiago Zanella-Béguelin. 2014. Probabilistic relational verification for cryptographic implementations. In *ACM SIGPLAN Notices*, Vol. 49. ACM, 193–205.

Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, and Santiago Zanella Béguelin. 2011. Computer-aided security proofs for the working cryptographer. In *Annual Cryptology Conference*. Springer, 71–90.

Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. 2009. Formal certification of code-based cryptographic proofs. *ACM SIGPLAN Notices* 44, 1 (2009), 90–101.

Bruno Blanchet. 2005. ProVerif automatic cryptographic protocol verifier user manual. *CNRS, Departement dInformatique, Ecole Normale Superieure, Paris* (2005).

Bruno Blanchet. 2007. CryptoVerif: Computationally sound mechanized prover for cryptographic protocols. In *Dagstuhl seminar âĂIJFormal Protocol Verification Applied*. 117.

Ran Canetti. 2001. Universally composable security: A new paradigm for cryptographic protocols. In *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*. IEEE, 136–145.

Ran Canetti and Marc Fischlin. 2001. Universally composable commitments. In *Annual International Cryptology Conference*. Springer, 19–40.

Jeffrey R Lewis and Brad Martin. 2003. Cryptol: High assurance, retargetable crypto development and validation. In *Military Communications Conference, 2003. MILCOM'03. 2003 IEEE*, Vol. 2. IEEE, 820–825.

A APPENDIX

Text of appendix …