An Efficient Deniable Key Exchange Protocol

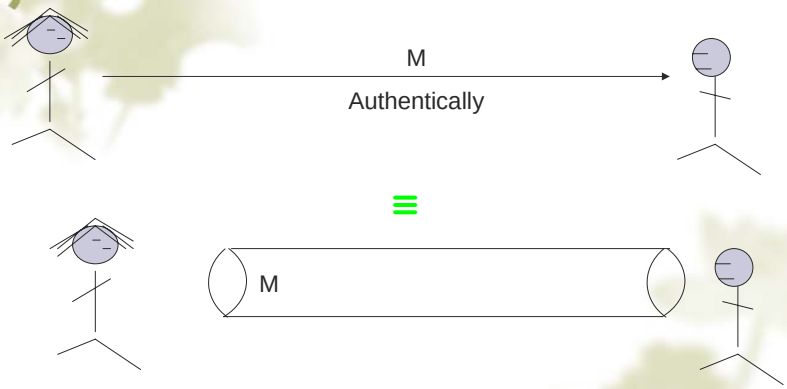
Shaoquan Jiang and Rei Safavi-Naini

University of Calgary

Special Thanks to Prof. Yvo Desmedt for Presenting the Paper.

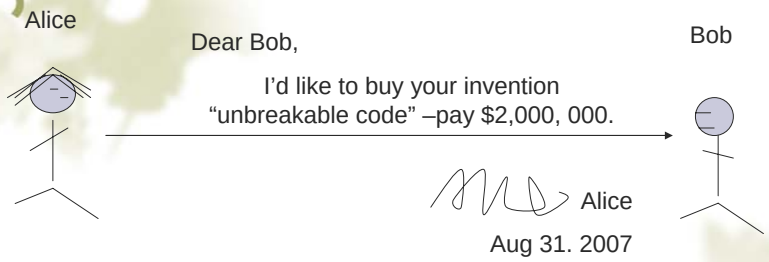
UNIVERSITY OF CALGARY

Authentication



M is authenticated if it is equivalent to the scenario where there is a message pipe between the sender and the receiver.

Authentication by digital signature

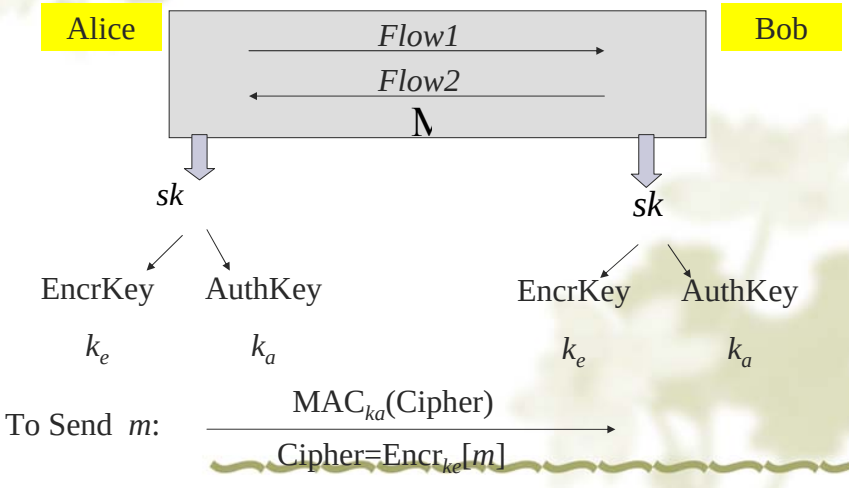


Drawback:

Digital signature is unforgeable. Everybody can verify authenticity of the signed message ➔ Alice can not deny. However, this undeniability is **not always desired**.

Secure Communication[CK01]

A common approach to secure communication is:
key exchange+Encryption-then-MAC.
Encryption-then-MAC is a shared key system. We consider *deniable key exchange*.



Previous Results

• Deniable Authentication was initiated in [DDN91] and formally in [DNS98]

• Security model for key exchange was proposed by Bellare and Rogaway [BR93]

• Deniable key exchange was informally discussed by Mao and Paterson [MP 02].

• Deniable key exchange with a formal proof was obtained in [DGK06]. They proved that SKEME is deniable in the sense of simulatability [DNS98]

• Deniable key exchange with a formal proof was also obtained in [Jiang07]. He showed a deniable authenticator theorem, which essentially states that if a protocol prot1 is deniably secure in the authenticated-link model (AM), then one can transform it into deniably secure in the unauthenticated-link model (UM) using *a deniable authenticator*. As the key exchange with no key (such as [JG05]) is deniably secure in AM, a deniably key exchange protocol can be obtained for a given deniable authenticator.

Our Results

In this work:

- We formalize a model for deniable key exchange by composing the key exchange model of Bellare-Rogaway [BR93] and Deniability of Dwork [DNS98].
- We propose a simple and efficient key exchange protocol and show it is deniably secure under the BR+DNS model above.

Adversary Model

Adversary attack is modeled using the following oracles.

Send(d, i, l_i, M):

Send a flow d message M to Instance l_i party i. This models Man-in-the-middle attack

Corrupt(i):

Corrupt party i and obtain his long term secret. This models the break-in attack.

Reveal(i, l_i)

Corrupt instance l_i and obtain its session key (if defined). This models the session key loss attack.

Test(i, l_i)

This is the security test. The adversary A chooses instance l_i in party i as a target. Then, he will receive a number w, which is either the session key of instance l_i or a random number. A is required to guess which is the case. Of course, Adversary should not break the partnered instance of l_i. He succeeds if the guess is correct.

Security Properties

• **Completeness.**

When there is no attack, then two parties share a session key.

• **Secrecy.**

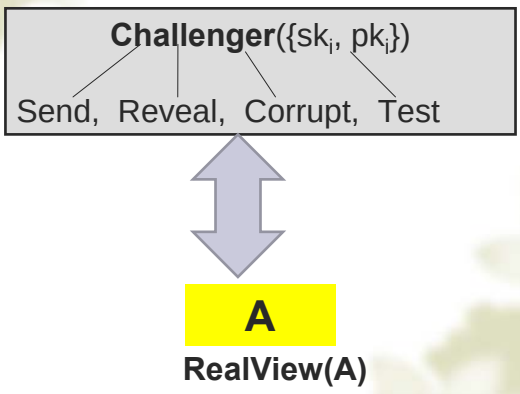
Adversary Success in **Test** Query is negligible.

• **Authentication**.

An instance successfully completes while no partnered instance in the assumed peer.

Deniability-Real Game

$\{sk_i, pk_i\} \leftarrow T(1^k)$ by a trusted party

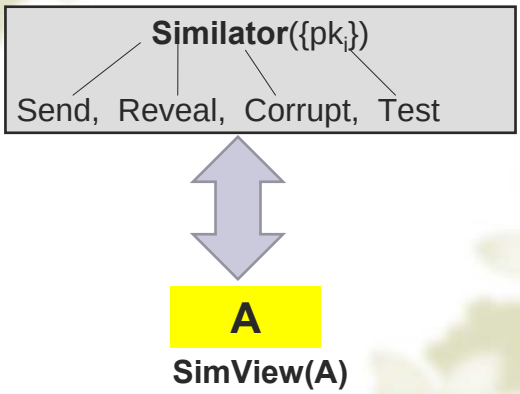


RealView(A)

A interacts with a challenger that uses $\{sk_i, pk_i\}$ to maintain oracles Finally, denote the view of A in this game by RealView(A).

Deniability—Simulated Game

$\{sk_i, pk_i\} \leftarrow T(1^k)$



SimView(A)

A interacts with a **Simulator** that uses {**pk**$_i$} to maintain oracles. Finally, denote the view of A in this game by SimView(A).

Deniability

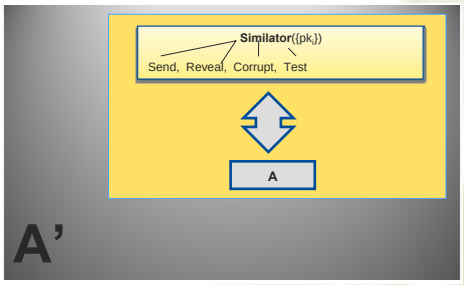
Definition of deniability

RealView(A)≈ SimView(A)

Why deniable?

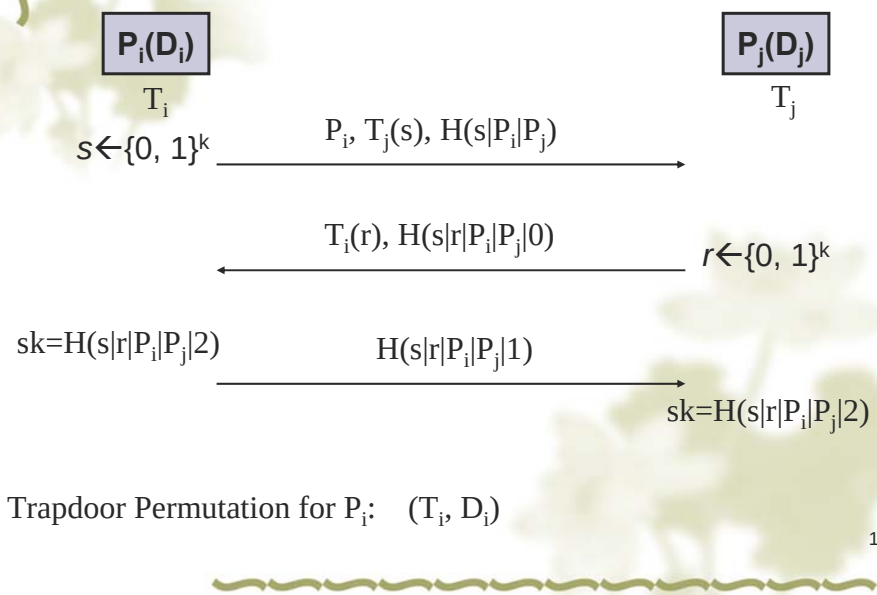
Given A and a simulator, an adversary can run A and simulator to obtain SimView(A) without interaction with honest parties.

SimView(A)



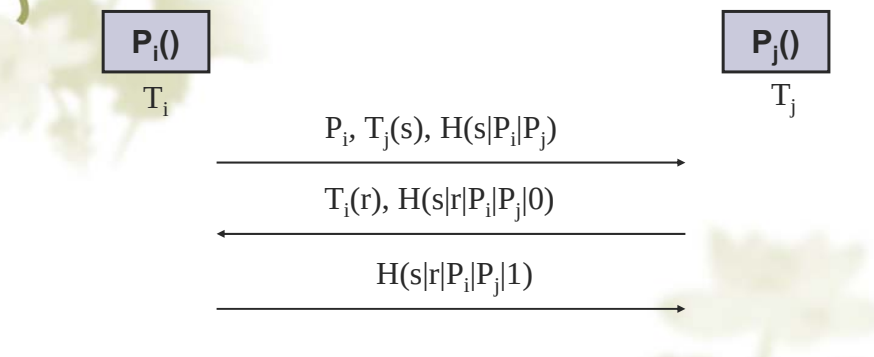
$\{sk_i, pk_i\} \leftarrow T(1^k)$

Our Protocol pRO-KE



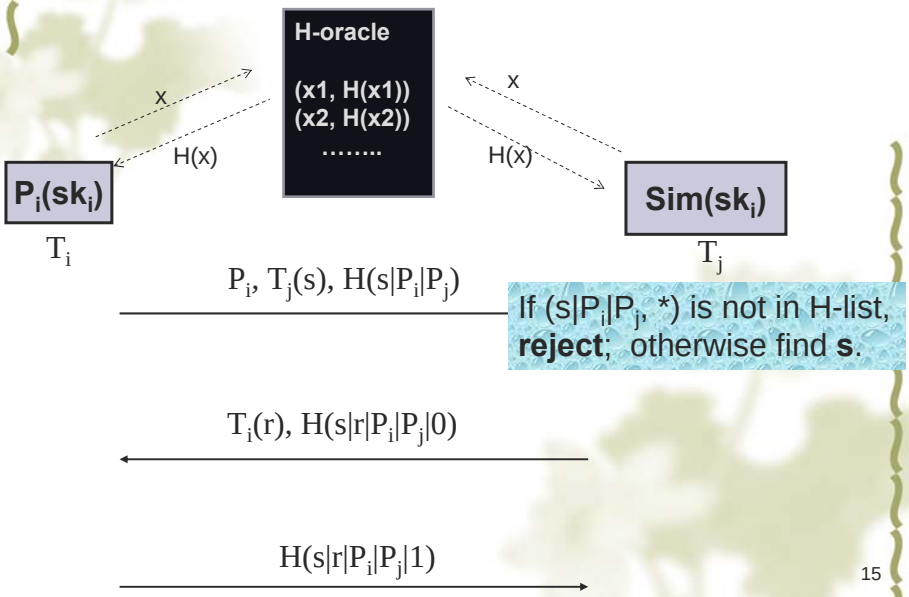
Trapdoor Permutation for P_i: (T_i, D_i)

Idea for why it is deniable: Eavesdropping



All **Send** queries can be simulated **without sk_i** and **sk_j** since s and r are taken by the *simulator*.

Idea for why it is deniable: P_i corrupted



Efficiency

Scheme	Comp Cost	Round Complexity	Worst Assumption	Instantiated Primitives
SKEME	6exps	3	KEA	Cramer-Shoup
uROE-KE	5exps	9	pRO	ElGamal and RSA
pRO-KE(this work)	2exps	3	pRO	RSA

Conclusion

In this work, we have the following result.

- We propose a new and deniable key exchange protocol
- It is proven deniably secure under the public random oracle model.
- It is more efficient than previous protocol of it kind.

Thank you and Questions!