A Security Proof for Key Exchange Protocol

Trieu Quang Phong
Nguyen Quoc Toan
Khuc Xuan Thanh

Institute of Cryptography Science and Technology
Gover. Info. Security Committee, Viet Nam

June 8, 2016

Our Works

- To study the security proof for key exchange protocols.
- More detail, to study the proof technique of C.Kudla and K.G.Paterson in [1], and apply it to prove the security of a concrete protocol.

The Technique of Kudla and Paterson

Theorem 5

Suppose that key exchange protocol Π produces a hashed session key on completion of the protocol (via hash function H) and that Π as strong partnering. If the cNR-mBR security of the related protocol π is probabilistic polynomial time reducible to the hardness of the computational problem of some relation f and the session string decisional problem for Π is polynomial time reducible to the decisional problem of f, then the mBR security of Π is probabilistic polynomial time reducible to the hardness of the Gap problem of f, assuming that H is a random oracle.

The Technique of Kudla and Paterson

For Π is the protocol that its session key is computed via a hash function. If Π satisfies the following conditions:

- Π has strong partnering.
- The security of **related protocol** π of Π is equivalent to the CDH problem.
- The DDH oracle can be used to solve the session string decisional problem of Π.

Then Π is secure by using the hardness of GDH problem.

Concrete Protocol

Π_A^i		Π_B^j
$role_A = initiator,\ pid_A = X_B$		$role_B = responder$
$a \in_R \mathbb{Z}_q,\ T_A = g^a \bmod p$	$T_A, X_A, X_B \rightarrow$	$pid_B = X_A$
		$b \in_R \mathbb{Z}_q,\ T_B = g^b \bmod p$
	$\leftarrow T_B, T_A, X_B, X_A$	$sid_B = X_A, X_B, T_A, T_B$
$sid_A = X_A, X_B, T_A, T_B$		$sk_B = H(T_A^{x_B} \bmod p, X_A^b \bmod p, sid_B)$
$sk_A = H(X_B^a \bmod p, T_B^{x_A} \bmod p, sid_A)$		

Figure 1. Protocol 1 in [1]

The Results of Protocol 1

Let Protocol 1' be the related protocol of Protocol 1.

Theorem 6 ([1], Theorem 3)

The cNR-mBR security of Protocol 1' is probabilistic polynomial time reducible to the hardness of the CDH problem in G.

Theorem 7 ([1], Theorem 4)

Protocol 1 has strong partnering in the random oracle model.

Corollary 8 ([1], Corollary 1)

Protocol 1 is secure in the random oracle model assuming the hardness of the Gap Diffie-Hellman problem.

Our Contribution

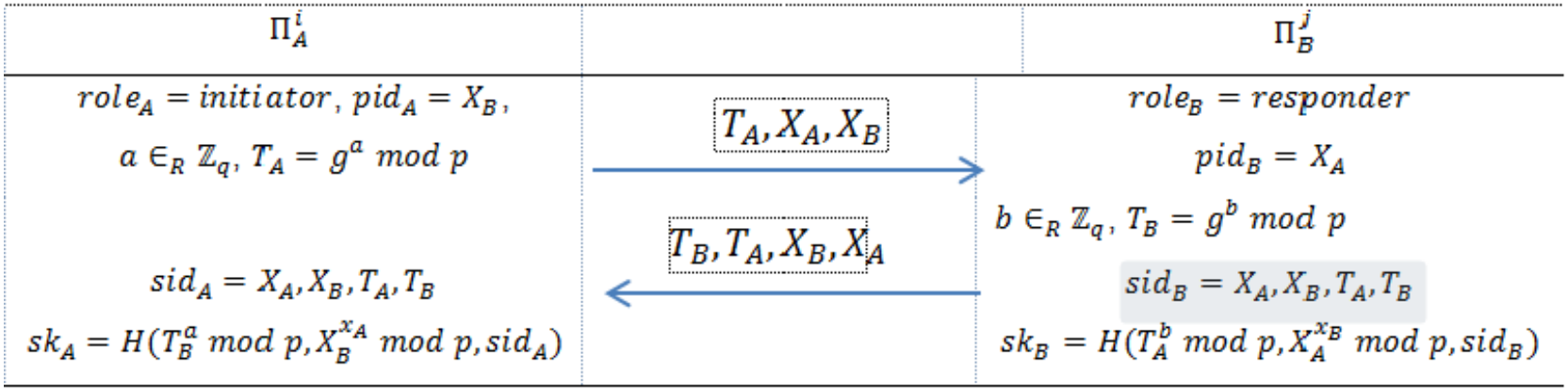

Figure 2. Protocol 2

Our Contribution

Let Protocol 2' be the related protocol of Protocol 2.

Theorem 9

The cNR-mBR security of Protocol 2' is probabilistic polynomial time reducible to the hardness of the CDH problem in G.

Theorem 10

Protocol 2 has strong partnering in the random oracle model.

Corollary 11

Protocol 2 is secure in the random oracle model assuming the hardness of the Gap Diffie-Hellman problem.

The Difference between Protocol 1 and Protocol 2

The session key of protocol 1:

$$H(g^{ax_B} \, modp, g^{bx_A} \, modp, X_A, X_B, T_A, T_B)$$

The session key of protocol 2:

$$H(g^{ab} \, modp, g^{x_A x_B} \, modp, X_A, X_B, T_A, T_B)$$

The Difference between Protocol 1 and Protocol 2

	Protocol $1'$	Protocol $2'$ (our modify)	Comment
The probability that $\mathcal{F}$ solves CDH on input (g^x, g^y) (where η is probability that E breaks the mBR-security)	$\frac{\eta}{n_P^2 \cdot n_S}$	$\frac{2\eta}{(n_P - 1)n_P \cdot n_S^2}$	According to these probability, the ability for reducing the mBR-security of Protocol $1'$ to the hardness of CDH is greater than that of Protocol $2'$

Table 1. The comparison of reduction probability.

Here,

- η is the probability which an adversary can break the the security of protocols.
- n_p is the number of participant.
- n_s is the is the maximal number of session at each participant.

Our Future Research

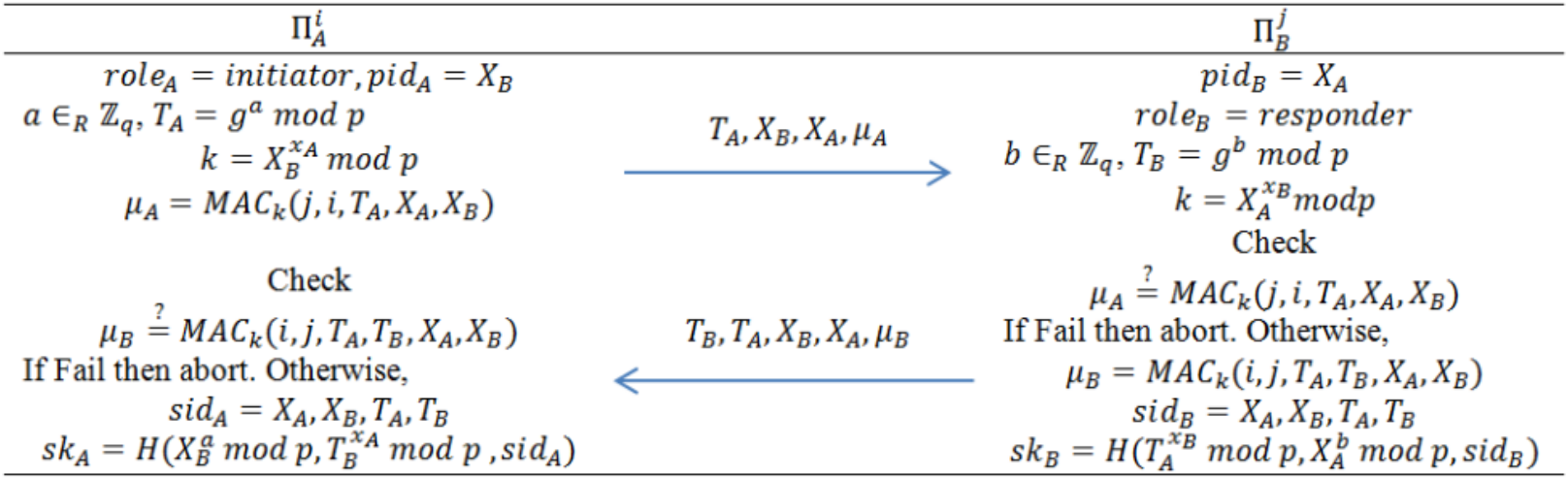

Figure 3. Protocol 3.

- To study key exchange protocols (eg. SIGMA, JFK, SESPAKE,...). And, we still have some indistinctness points in these protocols.

References

1. C. Kudla and K. G. Paterson. "Modular Security Proofs for Key Agreement Protocols". Advances in Cryptology ASIACRYPT05, pp. 549565, Springer-Verlag, 2005.
2. S. Blake-Wilson, D. Johnson, and A. Menezes. "Key agreement protocols and their security analysis". In Cryptography and Coding, volume 1355 of LNCS, pages 3045. Springer-Verlag, 1997.

Thanks for your listening!