Considering Two MAC under SIG Variants of The Basic SIGMA Protocol

Trieu Quang Phong

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

May 29, 2018

Content

Introduction

- The basic SIGMA protocol [3] is one of the authenticated Diffie-Hellman key exchange protocol based on the "sig-and-mac" mechanism and can be used in the IPsec standards.
- This protocol was proved secure on the in a variant of the CK (pre-specified peer) model [1] in that adapt to the setting where peer identities are not necessarily known or disclosed from the start of the protocol, namely the CK "post-specified peer" model [2].

Introduction

- The basic SIGMA protocol [3] is one of the authenticated Diffie-Hellman key exchange protocol based on the "sig-and-mac" mechanism and can be used in the IPsec standards.
- This protocol was proved secure on the in a variant of the CK (pre-specified peer) model [1] in that adapt to the setting where peer identities are not necessarily known or disclosed from the start of the protocol, namely the CK "post-specified peer" model [2].

Introduction

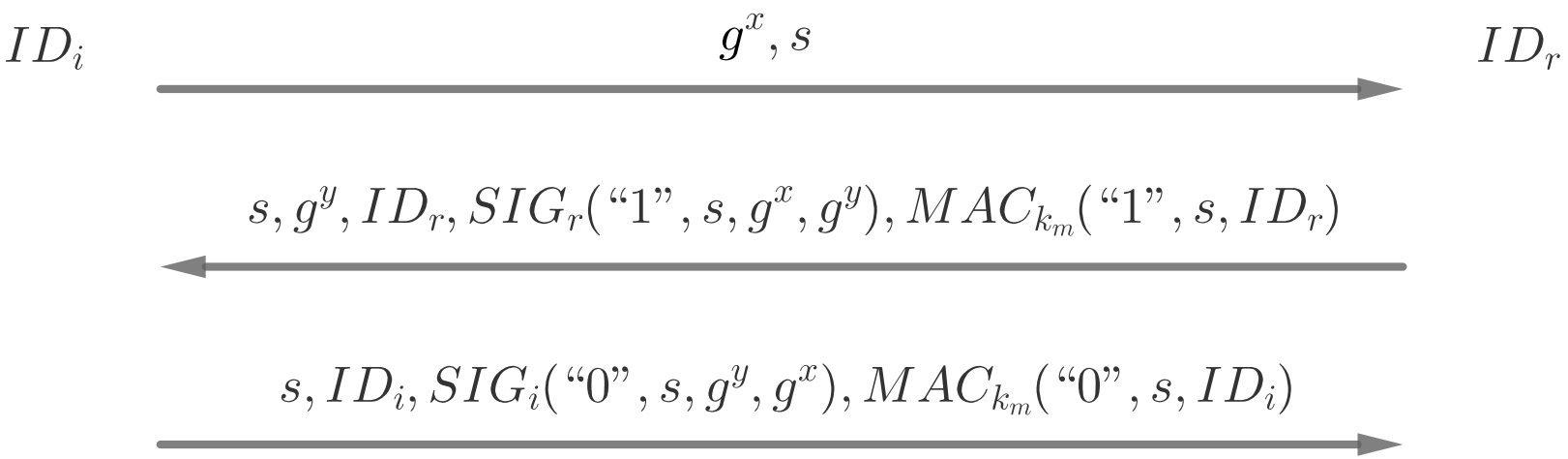

Figure 1. The basic SIGMA protocol

Introduction

There are some variants of the Basic SIGMA protocol in [3]:

- SIGMA-I
- SIGMA-R
- "full fledge" SIGMA

Introduction

There are some variants of the Basic SIGMA protocol in [3]:

- SIGMA-I
- SIGMA-R
- "full fledge" SIGMA

Introduction

There are some variants of the Basic SIGMA protocol in [3]:

- SIGMA-I
- SIGMA-R
- "full fledge" SIGMA

Introduction

There are some variants of the Basic SIGMA protocol in [3]:

- SIGMA-I
- SIGMA-R
- "full fledge" SIGMA

Introduction

Another variant of the Basic SIGMA protocol is proposed by R. Canetti and H. Krawczyk in [2].

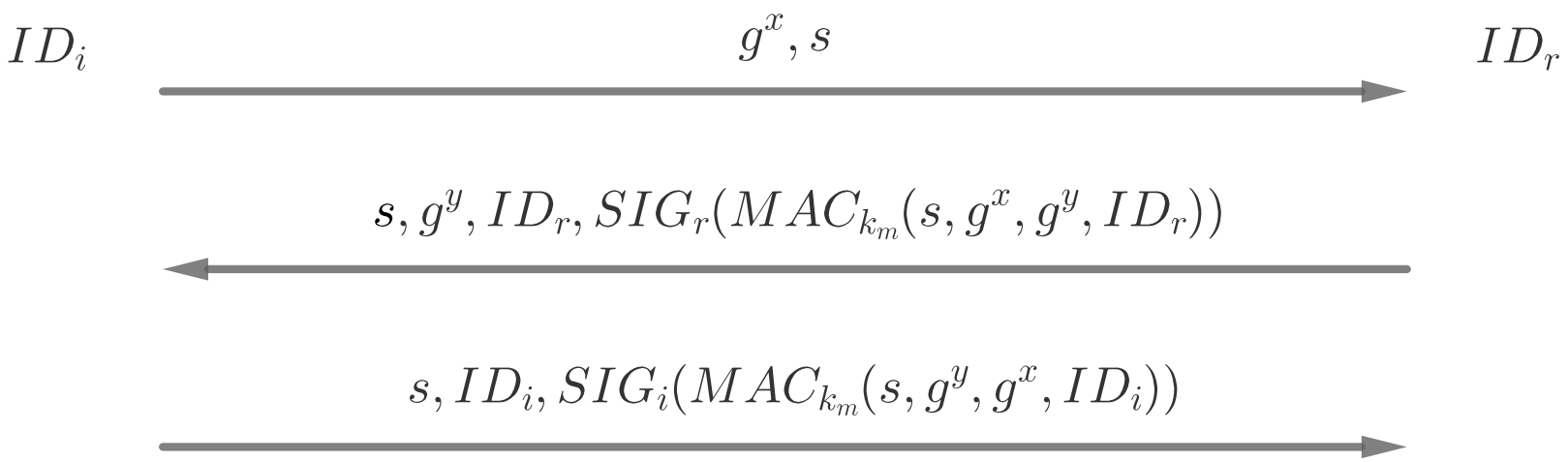

Figure 2. The variant of the basic SIGMA protocol that put the *MAC* under the signature

Introduction

According to [2], there are three advantages of this variant:

- To save the extra space taken by the *MAC* tag;
- To provide a message format consistent with other authentication modes of IKE.
- It is secure in the CK post-specified peer model.

$\Longrightarrow$ We are interested in studying this variant

Introduction

According to [2], there are three advantages of this variant:

- To save the extra space taken by the *MAC* tag;
- To provide a message format consistent with other authentication modes of IKE.
- It is secure in the CK post-specified peer model.

$\Longrightarrow$ We are interested in studying this variant

Introduction

According to [2], there are three advantages of this variant:

- To save the extra space taken by the *MAC* tag;
- To provide a message format consistent with other authentication modes of IKE.
- It is secure in the CK post-specified peer model.

$\Longrightarrow$ We are interested in studying this variant

Introduction

According to [2], there are three advantages of this variant:

- To save the extra space taken by the *MAC* tag;
- To provide a message format consistent with other authentication modes of IKE.
- It is secure in the CK post-specified peer model.

$\Longrightarrow$ We are interested in studying this variant

Introduction

According to [2], there are three advantages of this variant:

- To save the extra space taken by the *MAC* tag;
- To provide a message format consistent with other authentication modes of IKE.
- It is secure in the CK post-specified peer model.

$\Longrightarrow$ We are interested in studying this variant

Motivation

There are two requirements for a secure protocol Π in the CK post-specified peer model:

P1. If two uncorrupted parties complete matching sessions under the protocol Π then, except for a negligible probability, the session key output in these sessions is the same.

P2. No efficient attacker on the protocol Π can distinguish a real response to the test-session query from a random response with non-negligible advantage.

Motivation

R. Canetti and H. Krawczyk claimed that:

- The security proof of the protocol in Figure 2 is essentially analyzed the same as the basic SIGMA protocol.
- All the arguments in the proof of Basic SIGMA that based on the security of signatures remain valid in this case by using Lemma 17 in [2].

Motivation

Lemma 17 [2]

"If SIG is a secure signature scheme and MAC a secure message authentication function then it is infeasible for an attacker to find different messages M and M' such that for a randomly chosen secret MAC-key k_m the attacker an compute $SIG(MAC_{k_m}(M'))$ even after seeing $SIG(MAC_{k_m}(M))$."

Motivation

There are two issues when applying that lemma to analyze the requirement P1 for the protocol in Figure 2:

- There is only one MAC-key in the statement of that lemma, but if adversary use a "man-in-the-middle" attack then two (uncorrupted) parties will compute two different MAC-keys.
- The condition in Lemma 17 in [2] is that the MAC-key is a randomly chosen secret key and the attacker cannot chose it. Howerver, in a "man-in-the-middle" attack, the attacker knows the MAC-key of the responder.

Motivation

By these reasons, we see that:

- the analysis of this variant is quite complex;
- and need to find another solution.

Motivation

$$SIG_A(\text{“}c\text{”}, s, g^x, g^y), MAC_{k_M}(s, A) \not\rightarrow SIG_A(MAC_{k_M}(s, g^x, g^y, A))$$

Step 1 : $SIG_A(\text{“}c\text{”}, s, g^x, g^y, MAC_{k_M}(s, A))$

Step 2 : $SIG_A(\text{“}c\text{”}, g^x, g^y, MAC_{k_M}(s, A))$ where $c \in \{0, 1\}$

Motivation

As a consequence, we obtain two variants of the Basic SIGMA protocol, namely M-SIGMA and M1-SIGMA, satisfying:

- The *MAC* tag is also put under the signature;
- Their security proofs are essentially analyzed the same as the basic SIGMA protocol.

M-SIGMA

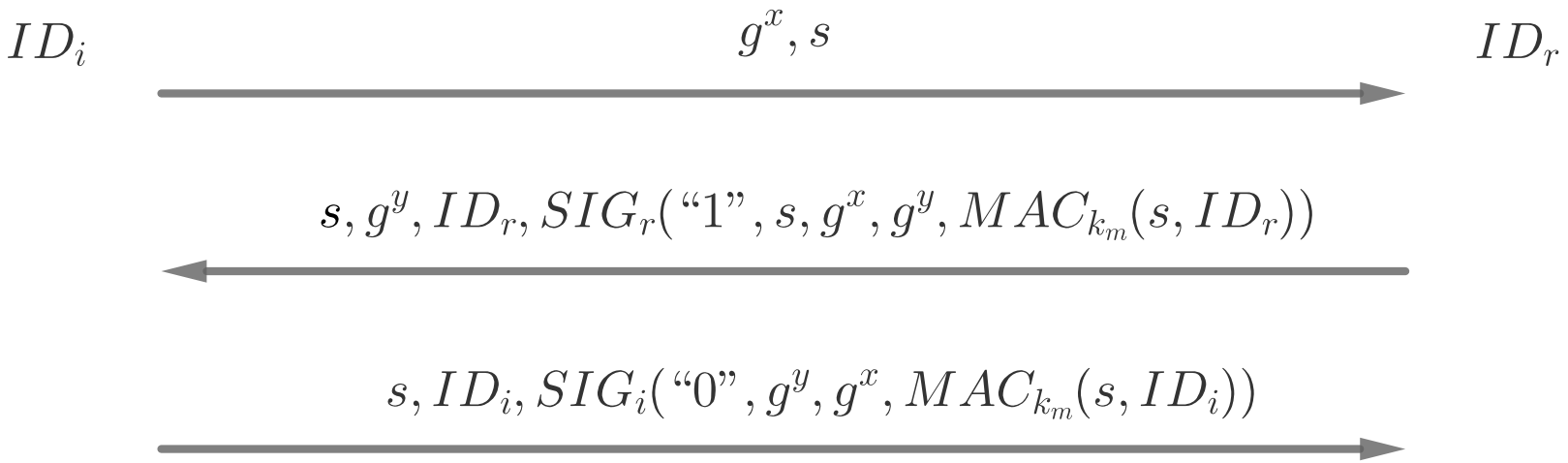

Figure 3. The M-SIGMA protocol

The difference between the security proofs for M-SIGMA and Basic SIGMA

For all attackers $\mathcal{M}$ on M-SIGMA, if a guess event happens under a run of $\hat{S}_{HYBR}(\mathcal{M})$ then the following properties hold (except for negligible probability):

(i) if (I_0, s_0) was chosen by $\mathcal{M}$ as the test session then (R_0, s_0) (either if completed or not) is its matching session;

(ii) if (R_0, s_0) was chosen by $\mathcal{M}$ as the test session then (I_0, s_0) is its matching session.

Result for M-SIGMA

Assuming DDH and the security of the underlying cryptographic functions *SIG*, *MAC*, *PRF*, the M-SIGMA protocol is secure in the Canetti-Krawczyk post-specified model.

M1-SIGMA

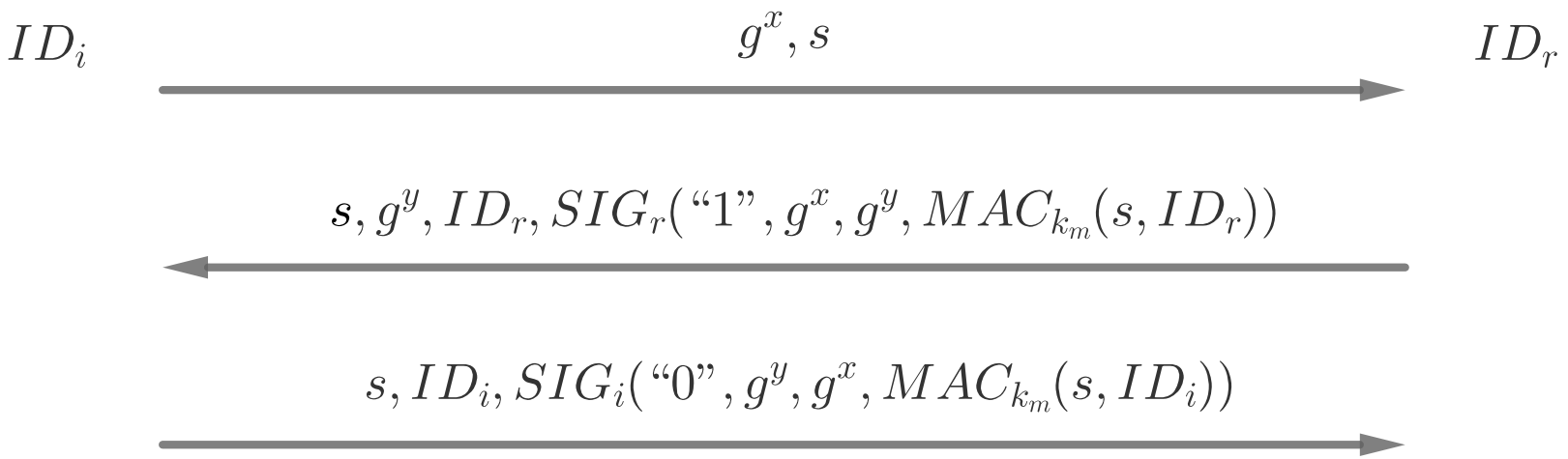

Figure 4. The M1-SIGMA protocol

The difference between the security proofs for M1-SIGMA and M-SIGMA

The M1-SIGMA protocol satisfies the first requirement of Definition 3.

For all attackers $\mathcal{M}$ on M1-SIGMA, the following holds except for negligible probability.

(a) Consider a regular run by $\mathcal{M}$ in which $\mathcal{M}$ chooses a test session with output $(\hat{A}, \hat{B}, s)$ where $\hat{A}$ is the initiator. Then:

(1) $\hat{A}$ and $\hat{B}$ are never corrupted before expiration of the test session.

(2) Sessions $(\hat{A}, s)$ and $(\hat{B}, s)$ are never revealed by $\mathcal{M}$.

(3) $(\hat{B}, s)$ is initiated as responder with the start message sent by $(\hat{A}, s)$.

...

Result for M1-SIGMA

Assuming DDH and the security of the underlying cryptographic functions *SIG*, *MAC*, *PRF*, the M1-SIGMA protocol is secure in the Canetti-Krawczyk post-specified model.

References


[1] R. Canetti and H. Krawczyk, Analysis of Key Echange Protocols and Their Use for Building Secure Channels, *Advances in Cryptology EUROCRYPT 2001*. `http://eprint.iacr.org/2001/040`.


[2] R. Canetti and H. Krawczyk, "Security Analysis of IKE's Signature-based Key-Exchange Protocol", *Crypto 2002*. LNCS Vol. 2442. Full version in: *Cryptology ePrint Archive at* `http://eprint.iacr.org/2002/120`.


[3] H. Krawczyk. SIGMA: The 'SIGn-and-MAc' approach to authenticated Diffie-Hellman and its use in the IKE protocols. *Annual International Cryptology Conference*. Springer, Berlin, Heidelberg, 2003.

Thanks for your listening!