SIGMA: the 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and its Use in the IKE Protocols

Hugo Krawczyk

IPsec meeting – Atlanta, Nov. 2002

Announcement of a new paper

SIGMA: the 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and its Use in the IKE Protocols

URL: `http://www.ee.technion.ac.il/~hugo/sigma.ps[.pdf]`

- A detailed presentation of the crypto rationale behind the design of the SIGMA family of key-exchange protocols
- Why should the IPsec WG care? Because
  - SIGMA is the protocol underlying the two IKE signature modes (main mode and aggressive mode)
  - SIGMA provides the cryptographic core and justification for IKEv2 Phase 1 key exchange (also JFK-r)

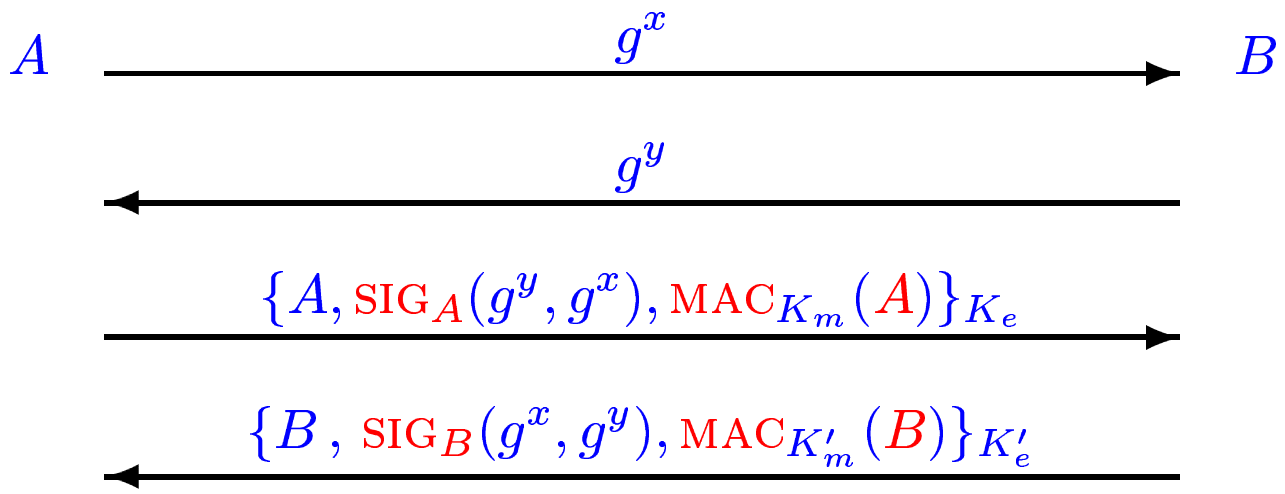
SIGMA and IPsec: historical context

- 94-95: Photuris the official key management protocol for IPsec
- 95: a serious security flaw in Photuris (with optional id prot): $\text{SIG}(g^x, g^y, g^{xy})$ (broken for RSA signatures) $\longrightarrow$ see paper
- suggested to replace the Photuris key-exchange with a new design (now named SIGMA)
- 96: IKE replaced Photuris, adopted the SIGMA exchange (main and aggressive signature modes)
- over the years many misunderstandings regarding the crypto rationale
  - including "rumours of insecurity" (beyond the famous IKE complexity and functionality issues)

The SIGMA paper

- SIGMA design process and rationale
  - technical but informal: directed to protocol designers and security engineers
- motivated by comparison to other protocols and attacks
- learn from strengths and weaknesses of previous protocols
- "sign the DH exponentials" $\not\Rightarrow$ authenticated DH exchange
- SIGMA: SIGn and MAc
  - the essential role of MACing the identity
    (a delicate issue in IKEv2)

Example: SIGMA-R



IKE signature main mode: MAC inside SIG: $\text{SIG}_A(\text{MAC}_{K_m}(A, g^y, g^x))$

IKEv2: MAC outside encryption $\overbrace{\{A, \text{SIG}_A(g^y, g^x)\}_{K_e}}$, $\text{MAC}_{K_m}(\cdots)$
(insecure if identity removed)

Swap messages 3 and 4: SIGMA-I (w/o encryption: aggressive mode)

SIGMA: some nice properties

- simple, minimal, efficient (computation and communication)
- perfect forward secrecy (PFS)
- supports id protection (I or R): but core security does not depend on it
- additional functionality can be added (do not forget to sign all what you send)
- DoS: orthogonal issue (either one of the "4 vs 6" solutions)
- formal analysis: Canetti and Krawczyk – Crypto'2002