ID-based authenticated key agreement Protokolle

30.11.2005

Ferdinand Jurczok

Überblick

- Warum ID-based key agreement?
  - Bsp.: Diffie-Hellman
  - Vor- / Nachteile
- Warum ID-based key agreement?
  - Bsp
  - Weil-Pairing
- Sicherheitsaspekte

Diffie-Hellman-Protokoll

- Eines der ersten key agreement Protokolle

Diffie-Hellman-Protokoll

- Eines der ersten key agreement Protokolle
- Sicherheit kann leicht durch man-in-the-middle Angriff gebrochen werden

Diffie-Hellman-Protokoll

- Eines der ersten key agreement Protokolle
- Sicherheit kann leicht durch man-in-the-middle Angriff gebrochen werden
- Lösung: authenticated key agreement (AK)

Diffie-Hellman-Protokoll

- Eines der ersten key agreement Protokolle
- Sicherheit kann leicht durch man-in-the-middle Angriff gebrochen werden
- Lösung: authenticated key agreement (AK)
- Problem: Nachrichten werden wesentlich länger als vorher

Diffie-Hellman-Protokoll

- Problem: Nachrichten werden wesentlich länger als vorher
- Lösung: z.B. MQV-Protokoll
  - Authentifizierung wird erreicht, ohne Größe und Anzahl der Nachrichten zu erhöhen

Diffie-Hellman-Protokoll

- Problem: Nachrichten werden wesentlich länger als vorher
- Lösung: z.B. MQV-Protokoll
  - Authentifizierung wird erreicht, ohne Größe und Anzahl der Nachrichten zu erhöhen
- Problem: Jede Partei muss die public keys aller anderen Parteien kennen
  - Hoher Speicheraufwand

ID-based Protokolle

- IDs jeder Partei dienen als public keys
- Trusted authority (TA) sorgt für Vergabe von private keys an die Parteien

1. Protokoll: N.P.Smart

- Benutzt (modifiziertes) Weil-Pairing
- Schritte:
  - Setup
  - Authentifizierter Schlüsselaustausch
- Effizienz: zwei Multiplikationen, zwei Auswertungen des Pairings

Sicherheitsaspekte

- Known key security
- Forward secrecy
- Key-compromise impersonation resilience
- Unknown key-share resilience
- Key control

2. Protokoll: L.Chen / C.Kudla

- Großenteils analog zu Smarts Protokoll, aber effektiver in der Berechnung der session keys

Ausblick

- Etliche Variationen der Protokolle vorstellbar

Ausblick

- Etliche Variationen der Protokolle vorstellbar
  - Mehrere TAs

Ausblick

- Etliche Variationen der Protokolle vorstellbar
  - Mehrere TAs
  - (Beliebig) viele Parteien

Ausblick

- Etliche Variationen der Protokolle vorstellbar
  - Mehrere TAs
  - (Beliebig) viele Parteien
  - ...
  - (to be continued)