SPOKE

Michel Abdalla - Fabrice Ben Hamouda - **David Pointcheval**
ENS - CNRS - INRIA

Crypto 2014 - Rump Session
Santa-Barbara, CA, USA - August 19th, 2014

PAKE

- **AKE:** Authenticated Key Exchange
  - allows two players to agree on a common key
  - authentication of partners
- **PAKE:** Password-Authenticated Key Exchange
  - authentication means: a short password
  - best attack: on-line dictionary attack
    (one test-password per active execution)

PAKE Protocols

- **EKE: Encrypted Key Exchange** [Bellovin-Merritt S&P92]
  - quite efficient but requires ***ideal cipher***
    - BPR-secure [Bellare-Pointcheval-Rogaway EC00] [Bresson-Chevassut-Pointcheval CCS03]
    - UC-secure [Abdalla-Catalano-Chevalier-Pointcheval CTRSA08]
  - **SPAKE**: BPR-secure variant in **ROM** [Abdalla-Pointcheval CTRSA05]
    - for *Simple Password-Authenticated Key Exchange*
- **KOY:** [Katz-Ostrovsky-Yung C01]
  - first candidate BPR-secure in the **standard model**
  - generalized by Gennaro-Lindell (EC03)
  - UC-secure variant [Canetti-Halevi-Katz-Lindell-MacKenzie EC05]

KOY/GL Framework

(Simplified)

$C_1 = \mathbf{E}_1(pw_C, r_1)$ →

← $C_2 = \mathbf{E}_2(pw_S, r_2)$, hp_2 (to verify C_1)

hp_1 (to verify C_2) →

Hash(hk_1,C_2) x **ProjHash**(hp_2,C_1,r_1)
= **ProjHash**(hp_1,C_2,r_2) x **Hash**(hk_2,C_1)

- **KOY: $\mathbf{E}_1 = \mathbf{E}_2$**
  - Cramer-Shoup encryption
- **GL: $\mathbf{E}_1 = \mathbf{E}_2$**
  - non-malleable commitment
  - instantiated with IND-CCA encryption

KOY/GL Framework

(Simplified)

$C_1 = \mathbf{E}_1(pw_C, r_1)$ →

$C_2 = \mathbf{E}_2(pw_S, r_2)$, hp_2 (to verify C_1) ←

hp_1 (to verify C_2) →

Hash(hk_1,C_2) x **ProjHash**(hp_2,C_1,r_1)
= **ProjHash**(hp_1,C_2,r_2) x **Hash**(hk_2,C_1)

- **KOY: $\mathbf{E}_1 = \mathbf{E}_2$**
  - Cramer-Shoup encryption
- **GL: $\mathbf{E}_1 = \mathbf{E}_2$**
  - non-malleable commitment
  - instantiated with IND-CCA encryption

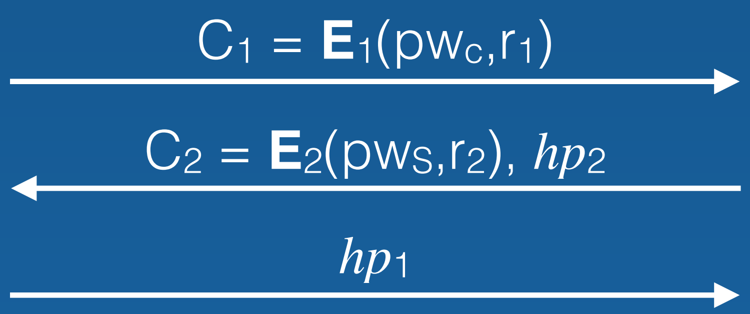
With both $\mathbf{E}_1 = \mathbf{E}_2$ = Cramer-Shoup encryption (**IND-CCA**):

$C_1 = C_2 = 4$ group elements

$hp_1 = hp_2 = 1$ group element

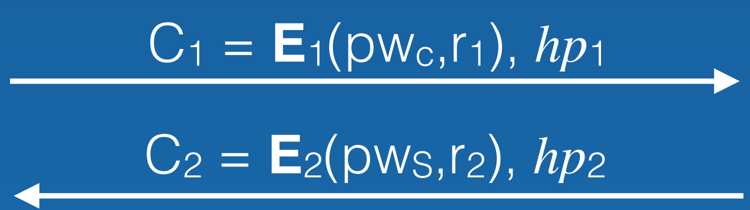
3 flows and 10 group elements + OT-Signature

Improvements



- $\mathbf{E}_2$ IND-CCA encryption
- $\mathbf{E}_1$ IND-**CPA** encryption

[Canetti-Halevi-Katz-Lindell-MacKenzie EC05]



With $\mathbf{E}_2$ = ElGamal encryption:

C_2 = 2 group elements

hp_1 = 1 group element

2 flows and no more OT-Signature

Improvements

$C_1 = \mathbf{E}_1(pw_C, r_1)$ →

← $C_2 = \mathbf{E}_2(pw_S, r_2)$, hp_2

hp_1 →

- $\mathbf{E}_2$ IND-CCA encryption
- $\mathbf{E}_1$ IND-**CPA** encryption

[Canetti-Halevi-Katz-Lindell-MacKenzie EC05]

$C_1 = \mathbf{E}_1(pw_C, r_1)$, hp_1 →

← $C_2 = \mathbf{E}_2(pw_S, r_2)$, hp_2

With $\mathbf{E}_2$ = ElGamal encryption:

C_2 = 2 group elements

hp_1 = 1 group element

2 flows and no more OT-Signature

- $\mathbf{E}_2$ IND-CPA encryption
- $\mathbf{E}_1$ IND-**PCA** encryption
  - Plaintext-Checking Attack

[Okamoto-Pointcheval CTRSA01]

Can we improve on C_1 and hp_2 ?

IND-PCA Variant

E$_1$ Cramer-Shoup Variant: $C = (u=g^r, e=h^r \text{ pw}, w=(cd^{\varepsilon})^r)$

$hk = (\alpha, \beta, \gamma)$ $\quad\quad hp = g^{\alpha} h^{\beta} (cd^{\varepsilon})^{\gamma}$

$H = u^{\alpha} (e/\text{pw})^{\beta} w^{\gamma}$ $\quad\quad H' = hp^r$ $\quad\quad$ **IND-PCA**

C_1 = 3 group elements

hp_2 = 1 group element

2 flows and 7 group elements

Final Protocol

Random r, α', β'

$(u=g^r, e=h^r \text{ pw}_a, w=(cd^{\varepsilon})^r), hp' = g^{\alpha'} h^{\beta'}$ →

← $(u'=g^{r'}, e'=h^{r'} \text{ pw}_b), hp = g^{\alpha} h^{\beta} (cd^{\varepsilon})^{\gamma}$

Random $r', \alpha, \beta, \gamma$

$hp^r \times u'^{\alpha'} (e'/\text{pw}_a)^{\beta'} = \text{SK} = u^{\alpha} (e/\text{pw}_b)^{\beta} w^{\gamma} \times hp'^{r'}$

Conclusion

- **Properties**
  - **The most efficient PAKE: 2 flows and 7 group elements**
  - Secure in the BPR setting
- **Bonus**: an efficient IND-PCA encryption scheme
- Applies to many **PAKE** protocols in the BPR setting:

1-round with 10 group elements

[Benhamouda-Blazy-Chevalier-Pointcheval-Vergnaud C13]

Available on **ePrint archive 2014/609**