

**Aspects of  
“Secret-Key Zero-Knowledge and  
Non-Interactive Verifiable  
Exponentiation”**

*Paper by Damgård and Cramer*

Karl Krukow

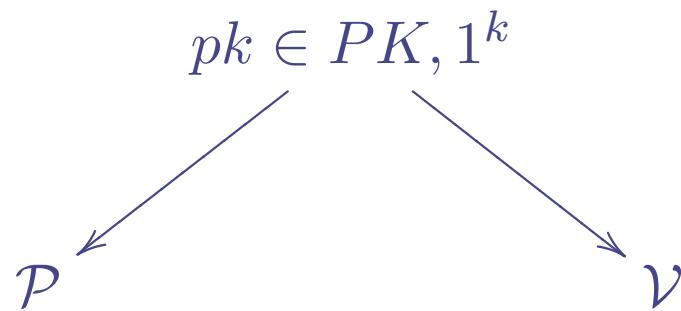
krukow@brics.dk

BRICS, University of Aarhus, Denmark

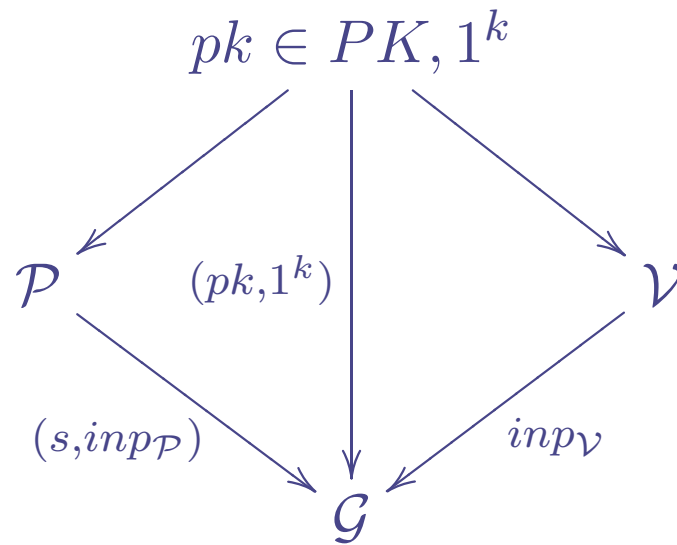
# Problem and Overview

- Problem: "... You're asked to do a brief presentation of the model, present the example based on discrete logarithms, and one or more examples of applications of the technique."
- Overview:
  - SKZKPS.
  - A DL-based SKZK proof system.
  - Application: Non-Interactive Verifiable Exponentiation
    - Shoup's RSA-threshold signatures.

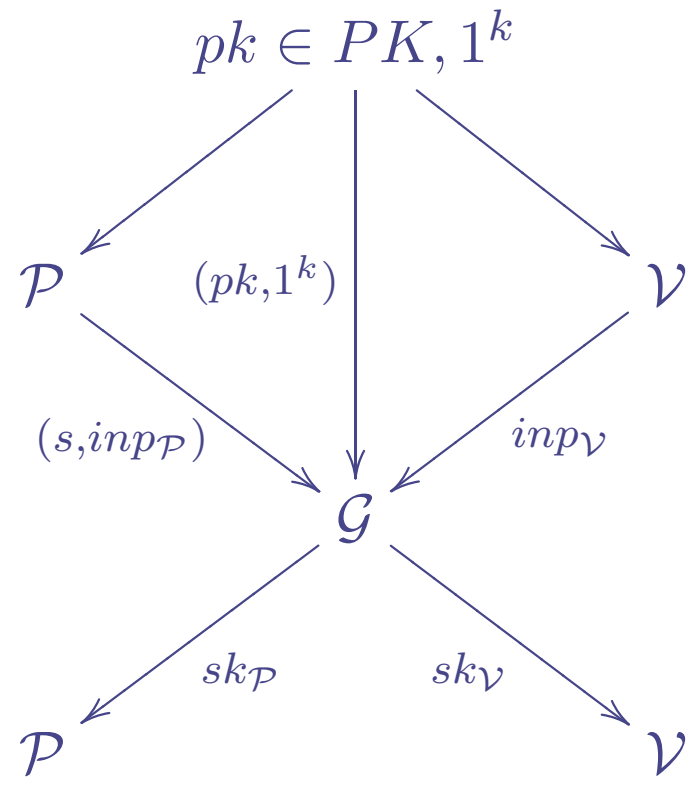
# SKZK: Set-up Phase



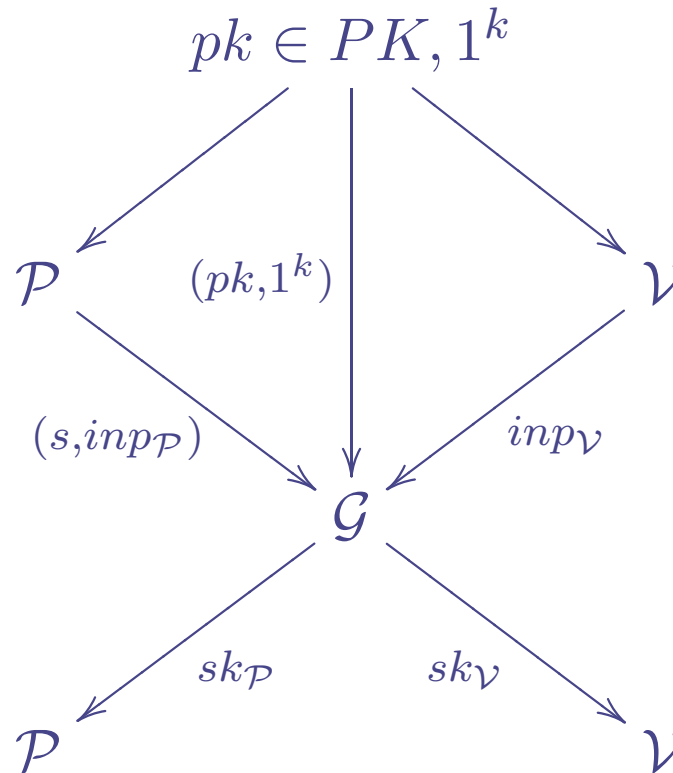
# SKZK: Set-up Phase



# SKZK: Set-up Phase

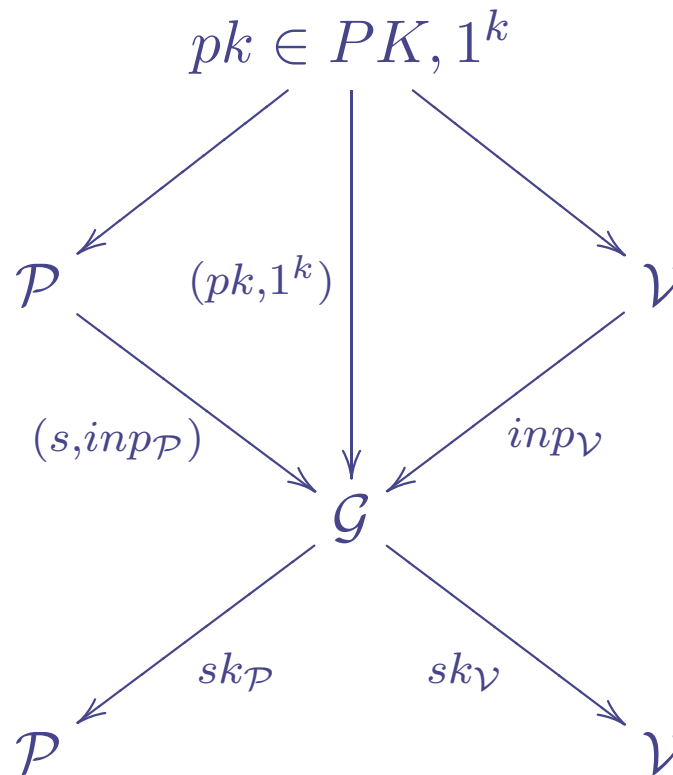


# SKZK: Set-up Phase



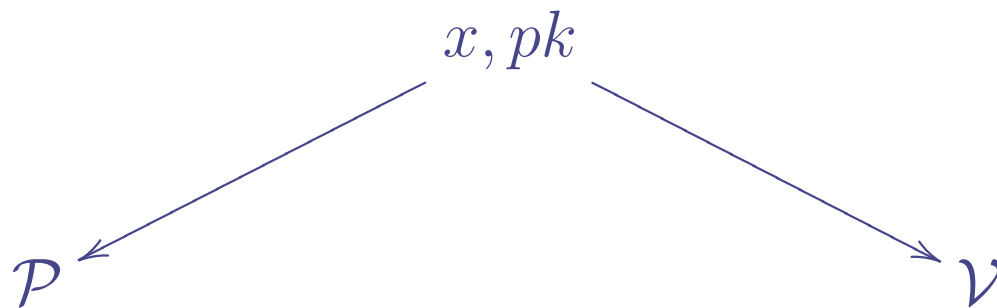
$(s, pk)$  determines a language  $L_{s,pk}$  for which membership is poly-time decidable given  $(s, pk)$ .

# SKZK: Set-up Phase

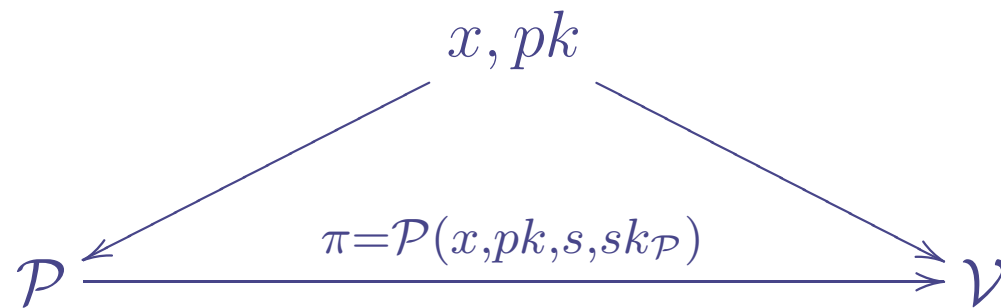


$(in_{\mathcal{P}}, in_{\mathcal{V}})$  models influence of prover/verifier on secret key generation.

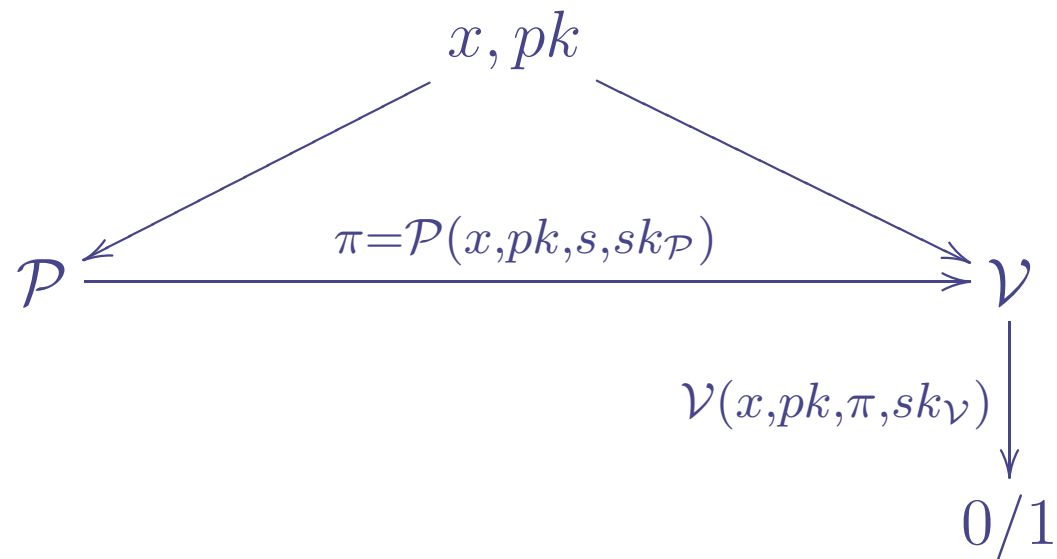
# SKZK: Proof-Phase



# SKZK: Proof-Phase



# SKZK: Proof-Phase



**Definition:** *The triple  $(\mathcal{G}, \mathcal{P}, \mathcal{V})$  is a secret-key zero-knowledge proof system (SKZKPS) for  $PK$  with error probability  $\epsilon(\cdot, -)$  if the following holds:*

**Definition:** *The triple  $(\mathcal{G}, \mathcal{P}, \mathcal{V})$  is a secret-key zero-knowledge proof system (SKZKPS) for  $PK$  with error probability  $\epsilon(\cdot, -)$  if the following holds:*

**Completeness:** *If  $x \in L_{s,pk}$  then  $\mathcal{V}$  accepts with probability 1.*

**Definition:** *The triple  $(\mathcal{G}, \mathcal{P}, \mathcal{V})$  is a secret-key zero-knowledge proof system (SKZKPS) for  $PK$  with error probability  $\epsilon(\cdot, -)$  if the following holds:*

**Completeness:** *If  $x \in L_{s,pk}$  then  $\mathcal{V}$  accepts with probability 1.*

**Soundness:** *For any prover  $P^*$  and any  $t$ , if  $P^*$  runs the set-up phase to get  $sk_{P^*}$ , and then adaptively creates  $t$  pairs  $(x_i, \pi_i)$ , then  $\mathcal{V}$  rejects all  $x_i \notin L_{s,pk}$  except with probability at most  $\epsilon(pk, t)$ .*

**Definition:** *The triple  $(\mathcal{G}, \mathcal{P}, \mathcal{V})$  is a secret-key zero-knowledge proof system (SKZKPS) for  $PK$  with error probability  $\epsilon(\cdot, -)$  if the following holds:*

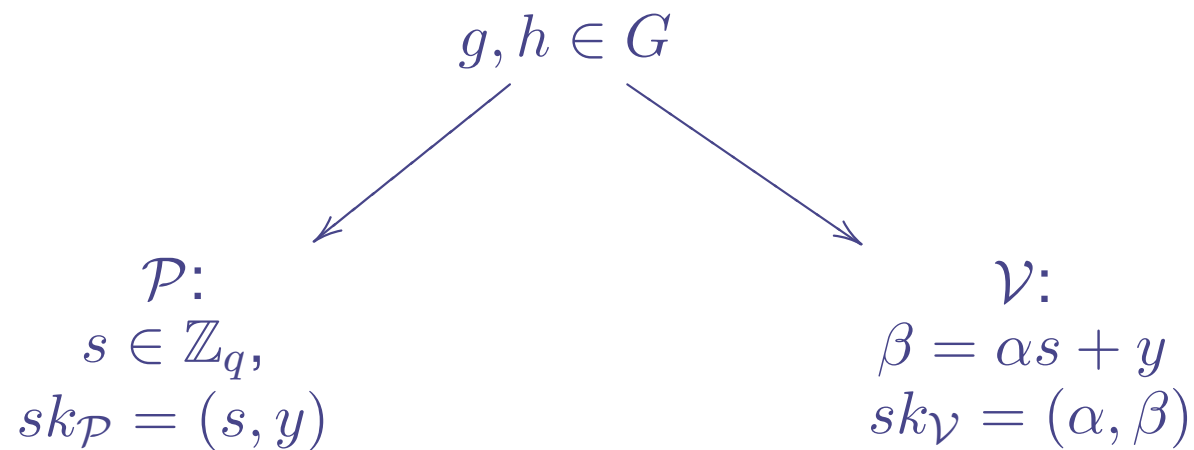
**Completeness:** *If  $x \in L_{s,pk}$  then  $\mathcal{V}$  accepts with probability 1.*

**Soundness:** *For any prover  $P^*$  and any  $t$ , if  $P^*$  runs the set-up phase to get  $sk_{P^*}$ , and then adaptively creates  $t$  pairs  $(x_i, \pi_i)$ , then  $\mathcal{V}$  rejects all  $x_i \notin L_{s,pk}$  except with probability at most  $\epsilon(pk, t)$ .*

**Zero-Knowledge:** *Any verifier  $V^*$ 's view of both key-generation and proofs of true statements can be efficiently simulated without access to  $\mathcal{P}$  or its information.*

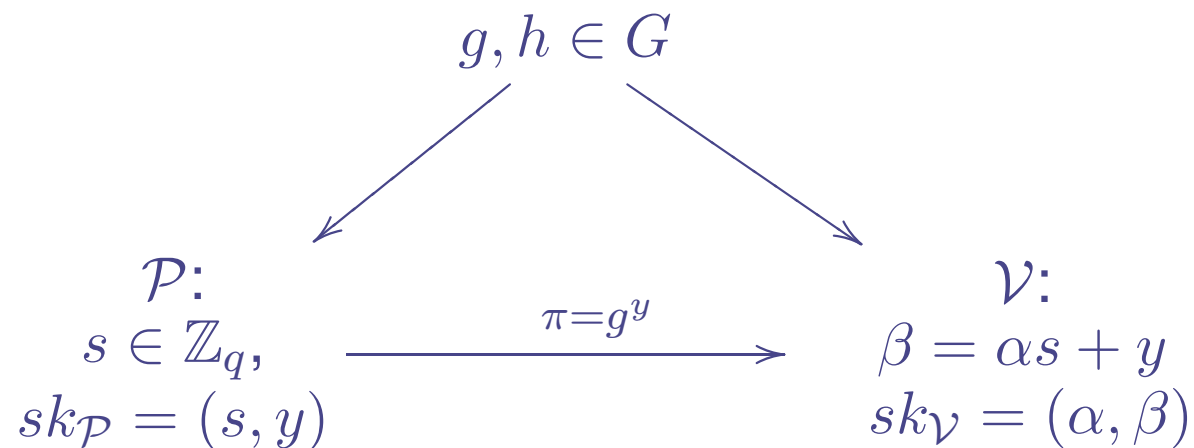
# Existence of SKZKs - preview

- Finite group  $G$  of prime order  $q$ , and that  $s \in \mathbb{Z}_q$  is fixed.
- $\mathcal{P}$  wants to convince  $\mathcal{V}$  that  $g, h$  satisfy  $h = g^s$ .
- Suppose  $sk_{\mathcal{P}}$  and  $sk_{\mathcal{V}}$  are magically set up:  $y, \alpha \in_R \mathbb{Z}_q$



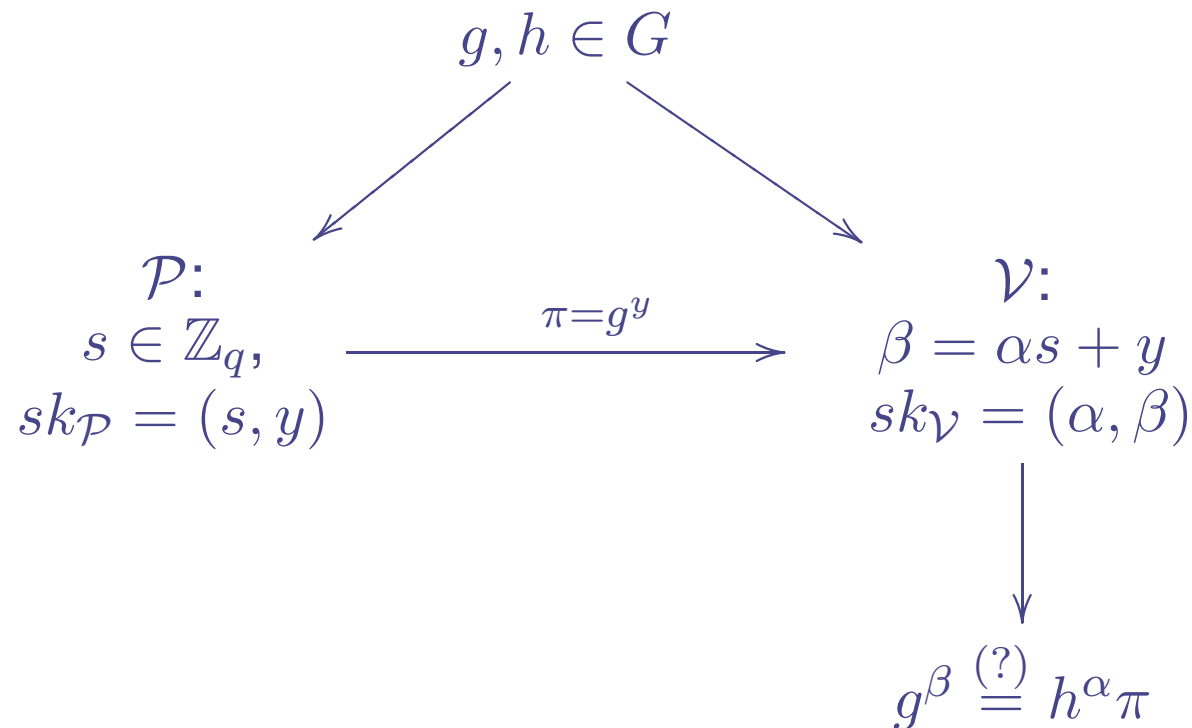
# Existence of SKZKs - preview

- Finite group  $G$  of prime order  $q$ , and that  $s \in \mathbb{Z}_q$  is fixed.
- $\mathcal{P}$  wants to convince  $\mathcal{V}$  that  $g, h$  satisfy  $h = g^s$ .
- Suppose  $sk_{\mathcal{P}}$  and  $sk_{\mathcal{V}}$  are magically set up:  $y, \alpha \in_R \mathbb{Z}_q$



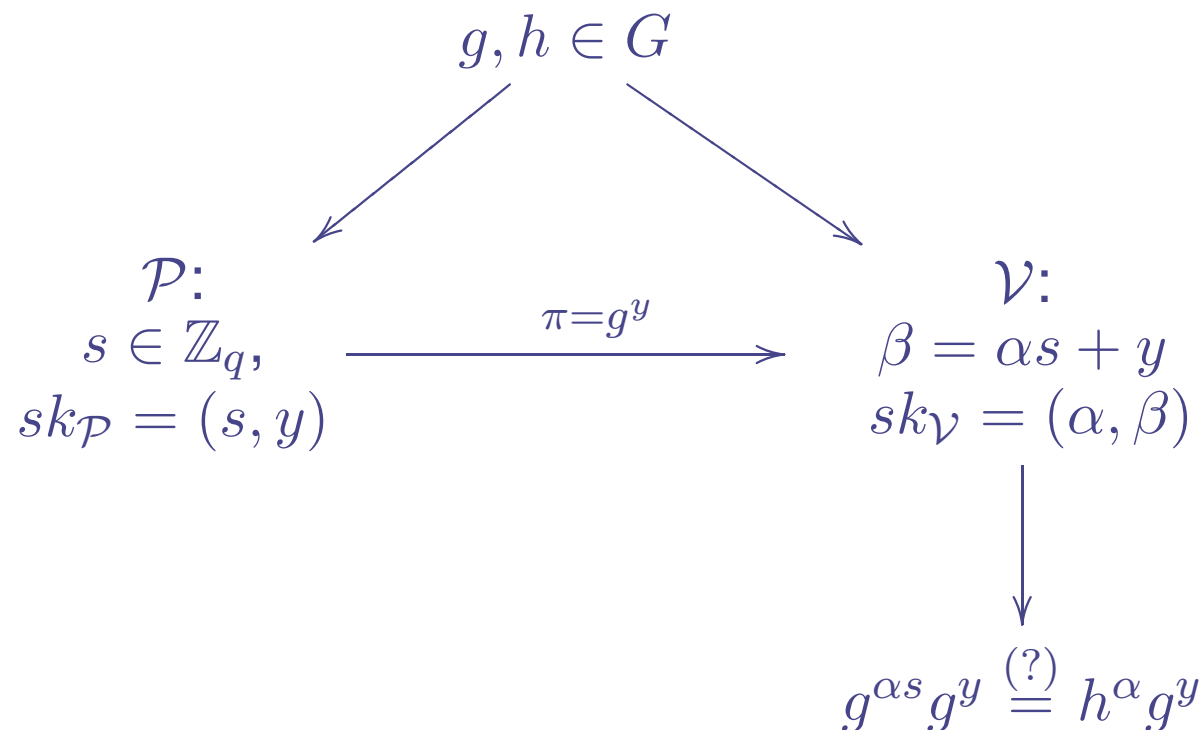
# Existence of SKZKs - preview

- Finite group  $G$  of prime order  $q$ , and that  $s \in \mathbb{Z}_q$  is fixed.
- $\mathcal{P}$  wants to convince  $\mathcal{V}$  that  $g, h$  satisfy  $h = g^s$ .
- Suppose  $sk_{\mathcal{P}}$  and  $sk_{\mathcal{V}}$  are magically set up:  $y, \alpha \in_R \mathbb{Z}_q$



# Existence of SKZKs - preview

- Finite group  $G$  of prime order  $q$ , and that  $s \in \mathbb{Z}_q$  is fixed.
- $\mathcal{P}$  wants to convince  $\mathcal{V}$  that  $g, h$  satisfy  $h = g^s$ .
- Suppose  $sk_{\mathcal{P}}$  and  $sk_{\mathcal{V}}$  are magically set up:  $y, \alpha \in_R \mathbb{Z}_q$



# Existence of SKZKs - Key Generation

- $PK$ : elements  $pk \in PK$  specifies a finite Abelian “computable” group  $G$  and two natural numbers  $k_0, k_1$ , where smallest prime factor of  $ord(G)$  is  $> 2^{k_0}$ .
- $L_{s,pk}$ : for  $pk$  and  $0 \leq s < 2^{k_1}$  ( $k_1$  bit string),  $L_{s,pk}$  are pairs  $g, h \in G$  with  $h = g^s$ .

# Existence of SKZKs - Key Generation

- $PK$ : elements  $pk \in PK$  specifies a finite Abelian “computable” group  $G$  and two natural numbers  $k_0, k_1$ , where smallest prime factor of  $ord(G)$  is  $> 2^{k_0}$ .
- $L_{s,pk}$ : for  $pk$  and  $0 \leq s < 2^{k_1}$  ( $k_1$  bit string),  $L_{s,pk}$  are pairs  $g, h \in G$  with  $h = g^s$ .
- $\mathcal{G}$ : on  $(G, k_0, k_1, k)$  and  $(s, inp_{\mathcal{P}}, inp_{\mathcal{V}})$ ,  $\mathcal{G}$  does:
  - test:  $0 \leq s < 2^{k_1}$ ,  $0 \leq inp_{\mathcal{P}} \leq 2^{k_0+k_1+k}$  and  $0 < inp_{\mathcal{V}} \leq 2^{k_0}$
  - $\alpha = inp_{\mathcal{V}}$  or  $\alpha \in_R ]0, 2^{k_0}]$
  - $y = inp_{\mathcal{P}}$  or  $y \in_R [0, 2^{k_0+k_1+k}]$
  - $\beta = \alpha s + y$
  - $sk_{\mathcal{V}} = (\alpha, \beta)$  and  $sk_{\mathcal{P}} = (s, y)$

# Existence of SKZK

**Theorem:**  $(\mathcal{G}, \mathcal{P}, \mathcal{V})$  as specified above is a SKZK proof system for PK with error probability  $\epsilon(k_0, t) = \frac{t}{2^{k_0-t}}$

# Existence of SKZK

**Theorem:**  $(\mathcal{G}, \mathcal{P}, \mathcal{V})$  as specified above is a SKZK proof system for PK with error probability  $\epsilon(k_0, t) = \frac{t}{2^{k_0-t}}$

*Proof.* (sketch)

- Completeness, just check.
- Soundness: assume for simplicity  $G$  is the subgroup of prime order  $q$  of  $\mathbb{Z}_p^*$  for safe prime  $p = 2q + 1$ . Proof can be done by induction in  $t$ .

# Existence of SKZK - Soundness

- Base,  $t = 1$ . Claim: If  $P^*$  can fake a proof, then it can determine  $\alpha$ .
- Let  $(g, h) \notin L_{s,pk}$ , i.e.  $h \neq g^s$ , and  $a$  generate  $G$ .
- Write  $g = a^i$ ,  $h = a^j$  and  $\pi = a^m$ . Now honest  $V$  accepts iff  $g^\beta = h^\alpha \pi$  iff  $a^{i(\alpha s + y)} = a^{j\alpha} a^m$  iff

$$\alpha si + yi \equiv \alpha j + m \pmod{q} \iff \alpha \equiv (m - yi)(si - j)^{-1} \pmod{q}$$

# Existence of SKZK - Soundness

- Base,  $t = 1$ . Claim: If  $P^*$  can fake a proof, then it can determine  $\alpha$ .
- Let  $(g, h) \notin L_{s,pk}$ , i.e.  $h \neq g^s$ , and  $a$  generate  $G$ .
- Write  $g = a^i$ ,  $h = a^j$  and  $\pi = a^m$ . Now honest  $V$  accepts iff  $g^\beta = h^\alpha \pi$  iff  $a^{i(\alpha s + y)} = a^{j\alpha} a^m$  iff

$$\alpha si + yi \equiv \alpha j + m \pmod{q} \iff \alpha \equiv (m - yi)(si - j)^{-1} \pmod{q}$$

- For inductive step: From each message, in the worst case,  $P^*$  can exclude one value for  $\alpha$ .

# Existence of SKZK - Zero-Knowledge

Simulating key generation:  $\mathcal{M}_1(1^k, pk, inp_{V^*})$ :

- Choose  $\alpha$  as  $\mathcal{G}$  would. (Perfect simulation).
- Choose  $\beta \in_R \{0, 1, \dots, 2^{k_0+k_1+k}\}$ .

# Existence of SKZK - Zero-Knowledge

Simulating key generation:  $\mathcal{M}_1(1^k, pk, inp_{V^*})$ :

- Choose  $\alpha$  as  $\mathcal{G}$  would. (Perfect simulation).
- Choose  $\beta \in_R \{0, 1, \dots, 2^{k_0+k_1+k}\}$ .

$$\Pr(\beta_{SIM} = \beta_0) = \begin{cases} \frac{1}{2^{k_0+k_1+k}+1} & \text{if } \beta_0 \in \{0, 1, \dots, 2^{k_0+k_1+k}\} \\ 0 & \text{if } \beta_0 \notin \{0, 1, \dots, 2^{k_0+k_1+k}\} \end{cases}$$

# Existence of SKZK - Zero-Knowledge

Simulating key generation:  $\mathcal{M}_1(1^k, pk, inp_{V^*})$ :

- Choose  $\alpha$  as  $\mathcal{G}$  would. (Perfect simulation).
- Choose  $\beta \in_R \{0, 1, \dots, 2^{k_0+k_1+k}\}$ .

$$\Pr(\beta_{SIM} = \beta_0) = \begin{cases} \frac{1}{2^{k_0+k_1+k} + 1} & \text{if } \beta_0 \in \{0, 1, \dots, 2^{k_0+k_1+k}\} \\ 0 & \text{if } \beta_0 \notin \{0, 1, \dots, 2^{k_0+k_1+k}\} \end{cases}$$

$$\Pr(\beta_{REAL} = \beta_0) = \begin{cases} 0 & \text{if } 0 \leq \beta_0 < \alpha s \\ \frac{1}{2^{k_0+k_1+k} + 1} & \text{if } \alpha s \leq \beta_0 \leq \alpha s + 2^{k_0+k_1+k} \\ 0 & \text{if } \beta_0 > \alpha s + 2^{k_0+k_1+k} \end{cases}$$

# Applications of SKZK

- Non-interactive verifiable exponentiation.
  - A set  $S$  of  $l$  servers of which at most  $t$  are corrupt.
  - $S$  share secret integer  $d$ .
  - Client  $C$  specifies  $g \in G$  for a finite Abelian group.
  - $S$  allow  $C$  to compute  $g^d$  non-interactively.
- e.g. Shoup's threshold RSA signature scheme.

# Threshold RSA Signatures

- $n = pq$  RSA modulus,  $e$  public RSA exponent.
- $t < l/2$  and  $t + 1$  servers must join to sign a message:  $g \mapsto g^d$
- Assume servers are sharing integer  $d$ . Server  $S_i$  has share  $s_i$ .
- Client  $C$  wants  $x \in \mathbb{Z}_n^*$  signed.
- Each server should compute  $x_i = x^{2\Delta s_i}$  where  $\Delta$  is publicly known. Servers are required to send also a proof that this was done correctly.
  - Shoup's approach: Non-interactive version of Chaum & Pedersen's equality of discrete logs. Requires Random oracle model.

# Replace proofs with SKZK

- In sign-phase servers must provide proof that  $x_i = x^{2\Delta s_i}$ .
- Assume that client has secret key  $sk_C^i = (\alpha_i, \beta_i)$ , for each server  $S_i$  with secret key  $sk_{S_i} = (\Delta s_i, y_i)$  so that  $\beta_i = \alpha_i \Delta s_i + y_i$ .
- Now servers can prove non-interactively in ZK that  $x_i$  is  $x^2$  raised to the fixed  $\Delta s_i$ .
- This replaces a non-interactive DL-proof using hashing, and the resulting scheme is secure if standard RSA signature scheme is secure.

# Summary

- Presented a new model for non-interactive ZK, SKZK.
- Shown that SKZKs exists (DL-Based example).
- Applied DL-Based example to obtain secure RSA-threshold signing.