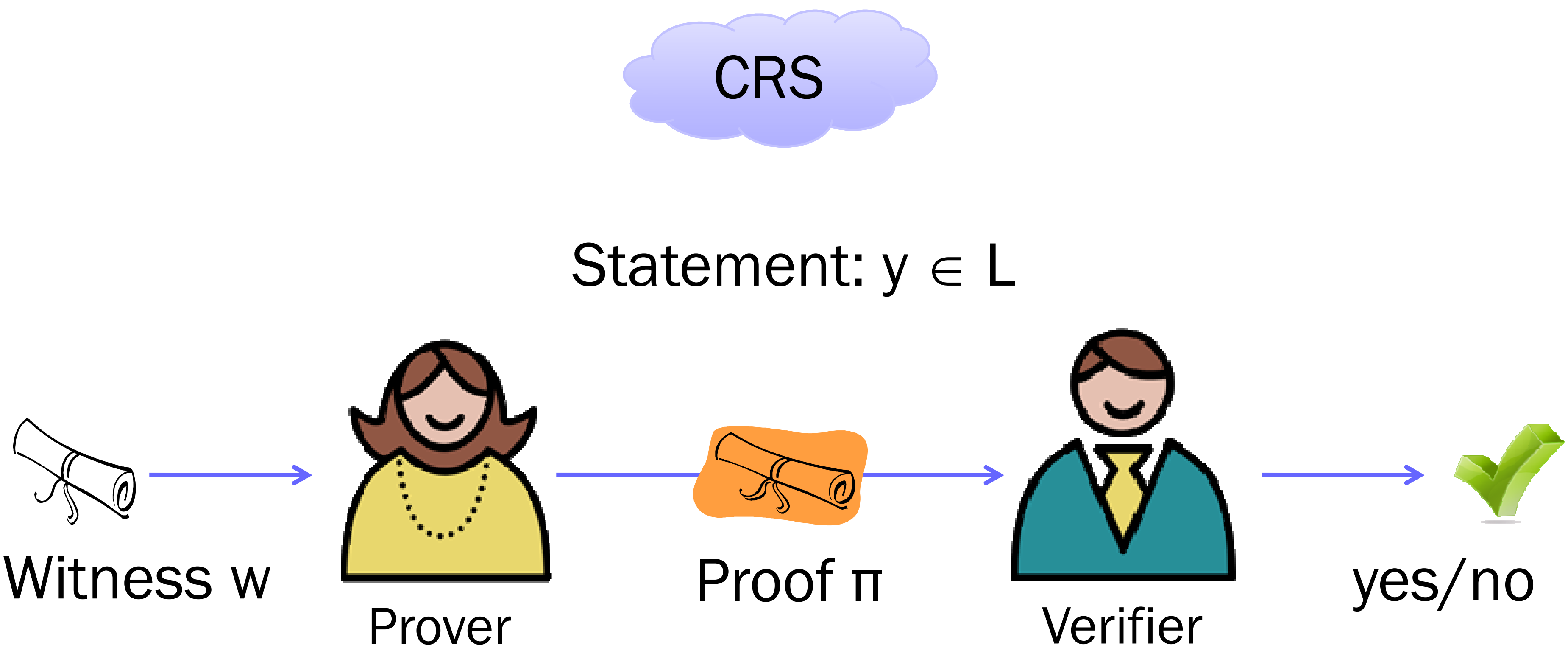
Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss,
Anna Lysyanskaya, and Hovav Shacham

# NON-INTERACTIVE RANDOMIZABLE PROOFS AND DELEGATABLE ANONYMOUS CREDENTIALS

# NON-INTERACTIVE ZERO KNOWLEDGE PROOFS

- Introduced, extended by [BDMP, FLS, KP, GOS]



# SECURITY PROPERTIES

- Completeness
  - Honest prover convinces verifier
- Soundness
  - No prover can convince verifier of false statement
- Zero Knowledge [GMR]
  - Proof reveals nothing besides truth of statement

# RANDOMIZABLE PROOFS

- New property: Randomizability
  - Randomized proof looks like freshly generated proof
- Additional algorithm: *randomize*

# OUR CONTRIBUTION

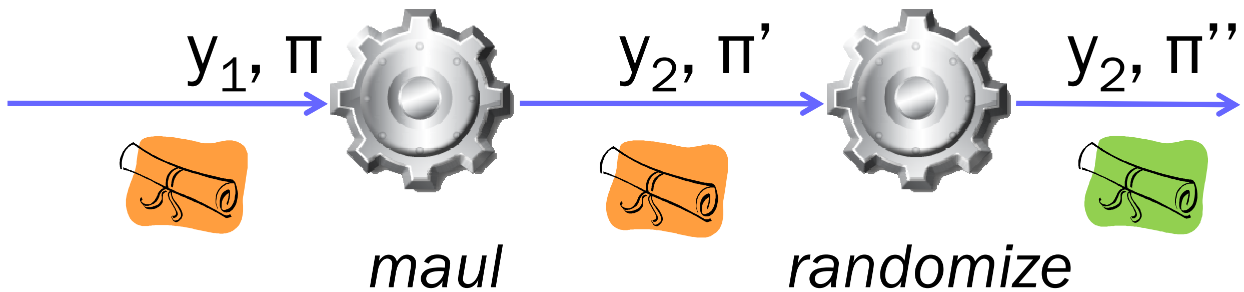
- Define randomizability
- Give randomizable NIZK proofs
  - for NP, building on [GOS]
  - leading to efficient applications building on [GS]

- Application: delegatable anonymous credentials

# RANDOMIZABILITY AND MALLEABILITY

- Malleability as a bug [DDN, Sahai, DDOPS]
- Malleability as a feature
  - Homomorphic encryption [ElGamal, Paillier, Gentry]
  - RCCA encryption [PR, Groth]
  - Translation between pseudonyms:

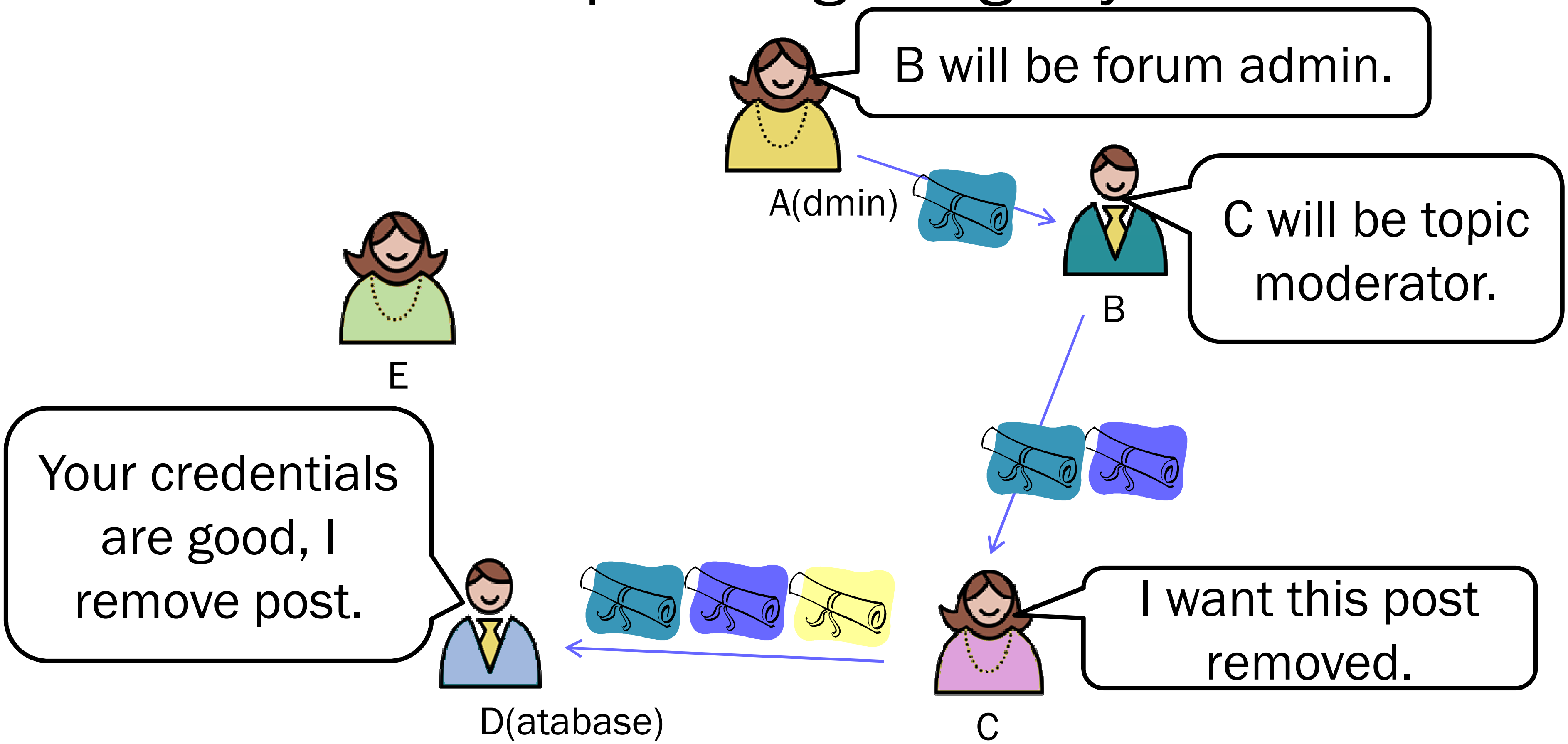
$y_1$ about $Nym_1 = Com(x, r_1)$, $y_2$ about $Nym_2 = Com(x, r_2)$




- proof $\pi''$ looks like fresh proof for $y_2$

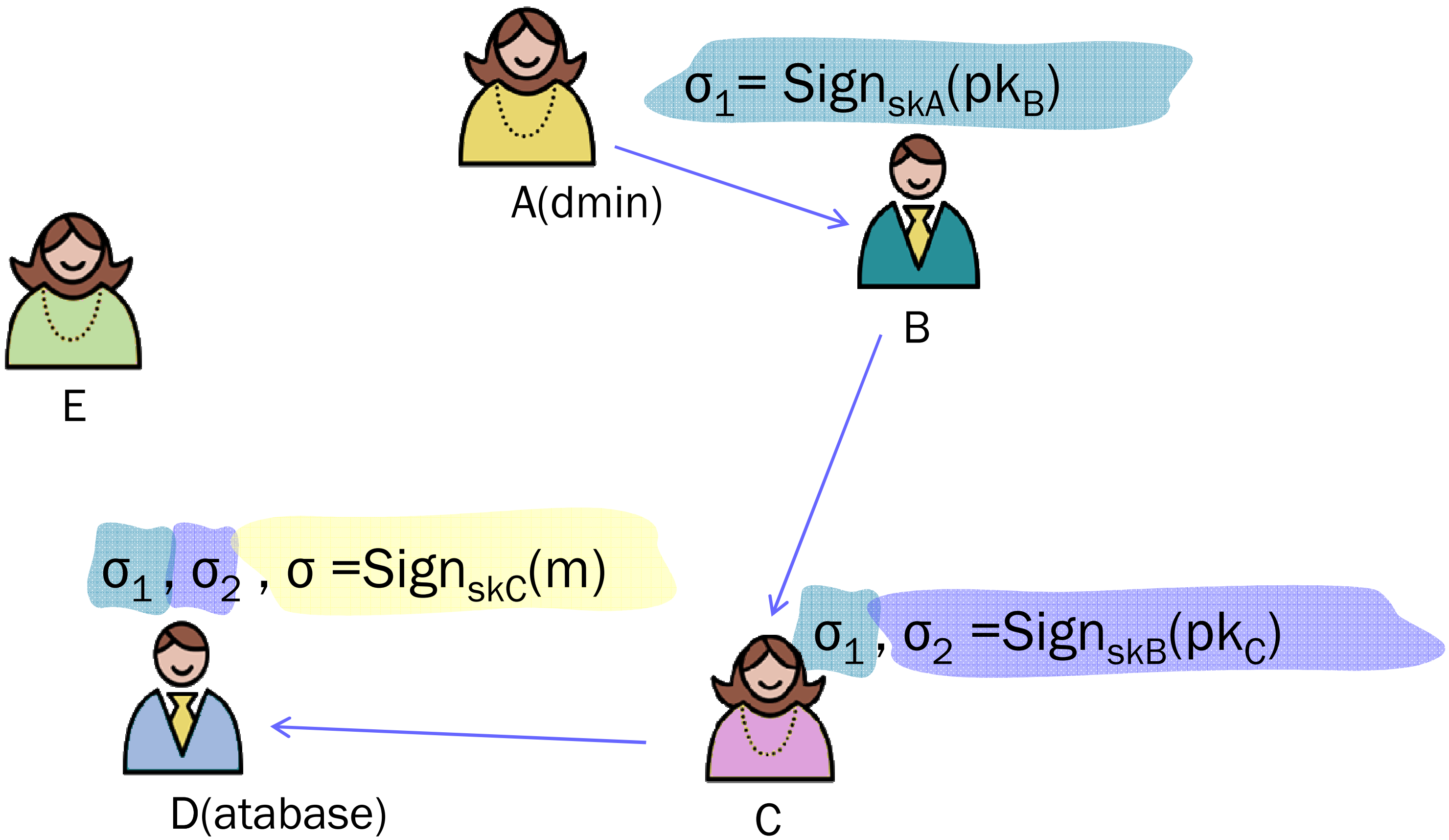
# DELEGATION OF CREDENTIALS

- Credentials help manage large systems.



# DELEGATION OF CREDENTIALS

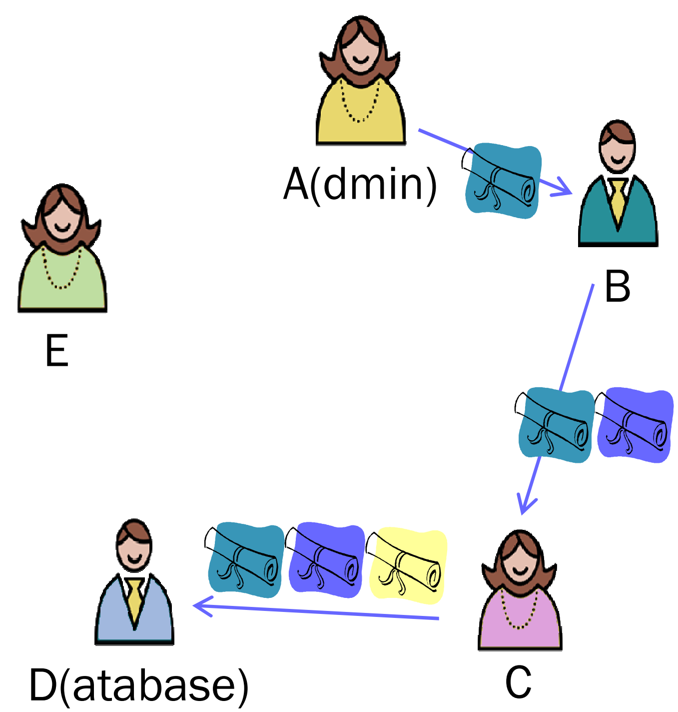
- Signatures → delegatable credentials



# DELEGATION AND PRIVACY

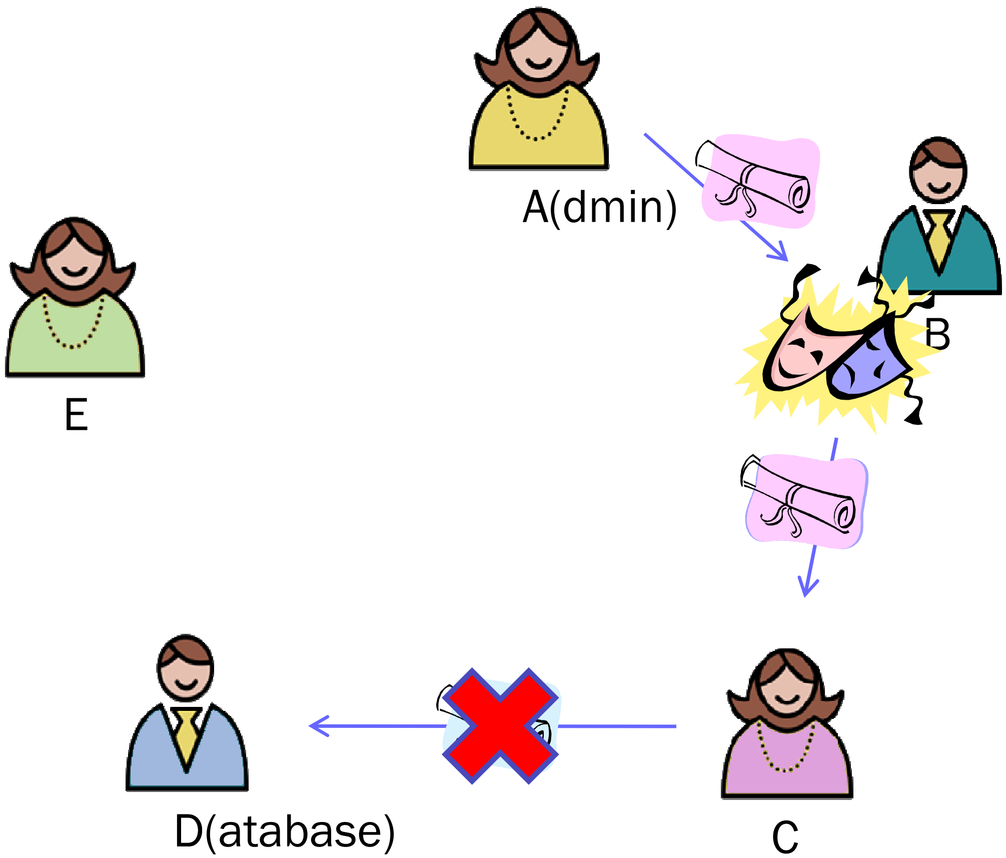
- Reveals sensitive information
- Should identification always be the default?
  - Controversial topics require a balanced system
  - flexible credential mechanisms (comparable to strong CCA, CMA definitions)

- Health care reforms
- Pro life vs. pro choice



# DELEGATION AND PRIVACY

- Anonymous credentials[Chaum, Brands, CLb]



# PRIOR WORK ON DELEGATABLE CREDENTIALS

- Non-interactive Meta-proofs [DY]
- Signatures of Knowledge [CLa]

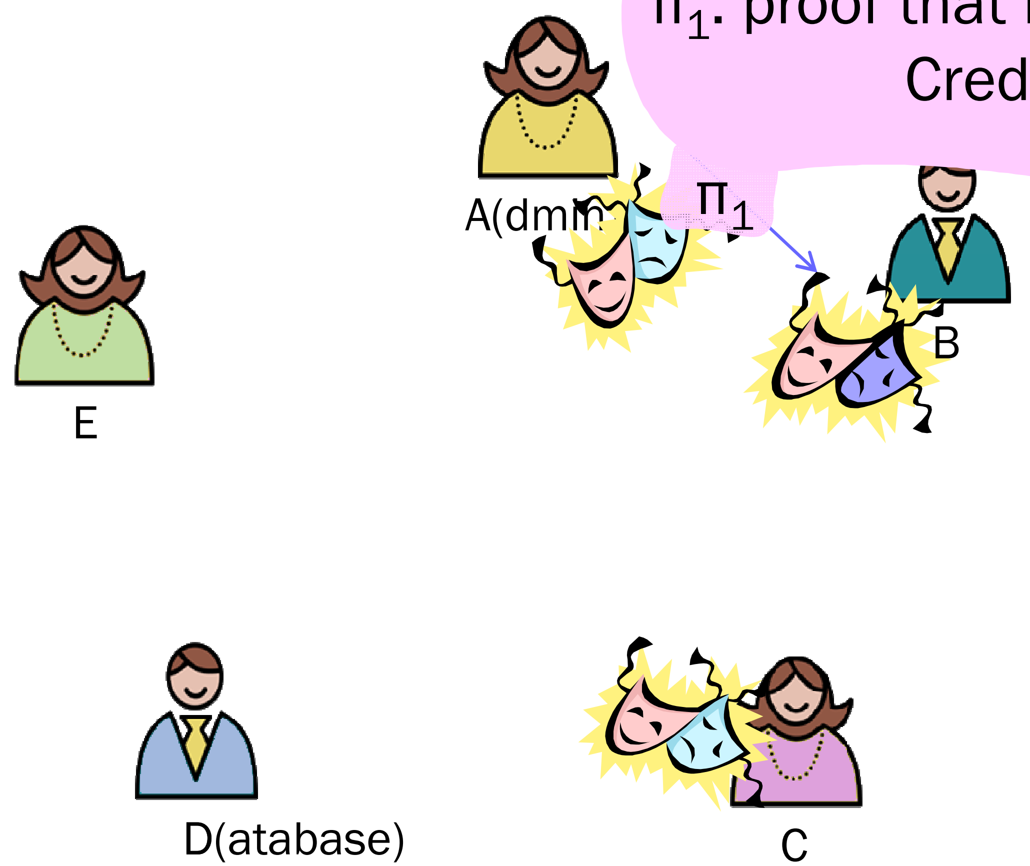
- Reduction to instances of circuit-SAT
- Proofs grow exponentially in number of levels

# DELEGATABLE ANONYMC

- Use randomizable proofs

NymA = Com(skA)
NymB = Com(skB)
Cred = Com($\sigma_{skA}$(skB))

$\pi_1$: proof that NymA, NymB and Cred correct



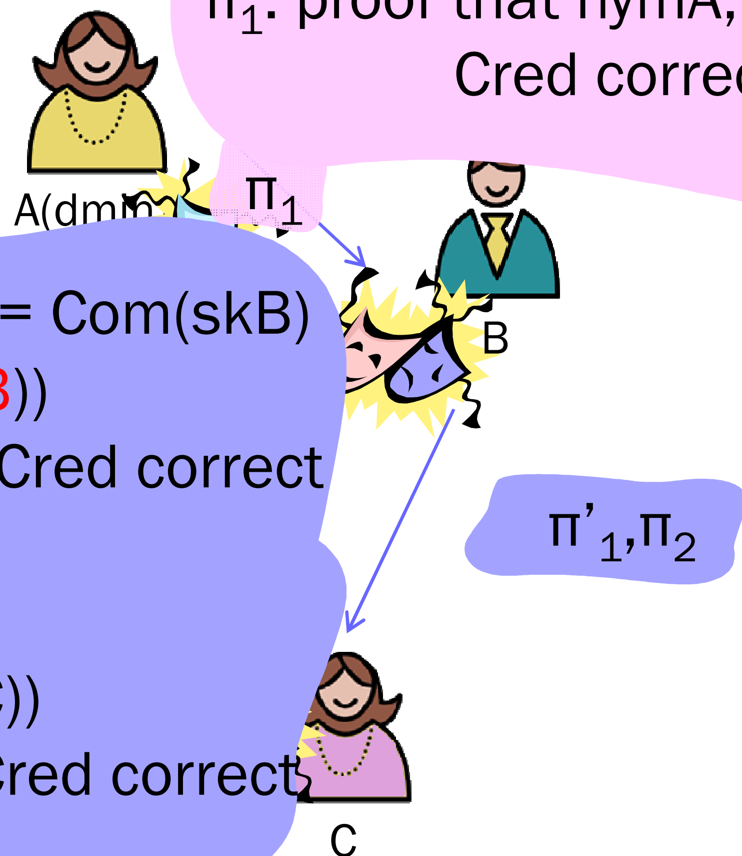
# DELEGATABLE ANONYMO

- Use randomizable proofs

*maul & randomize*

NymA = Com(skA)
NymB = Com(skB)
Cred = Com($\sigma_{skA}$(skB))

$\pi_1$: proof that nymA, NymB and Cred correct




NymA = Com(skA), NymB’ = Com(skB)
Cred’ = Com($\sigma_{skA}$(skB))
Proof $\pi'_1$: nymA, nymB’ and Cred correct

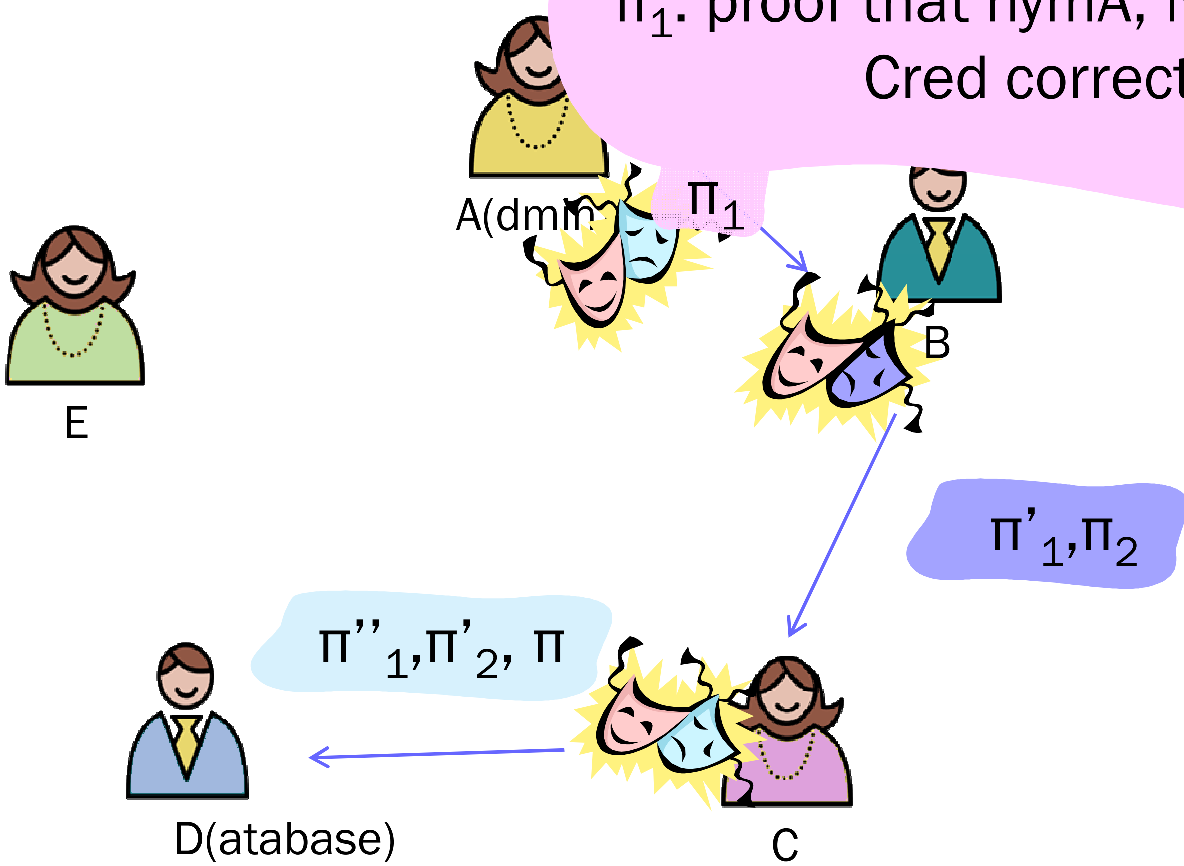
NymC = Com(skC)
Cred = Com($\sigma_{skB}$(skC))
Prove $\pi_2$ : nymB’, NymC and Cred correct

# DELEGATABLE ANONYM

- Use randomizable proo

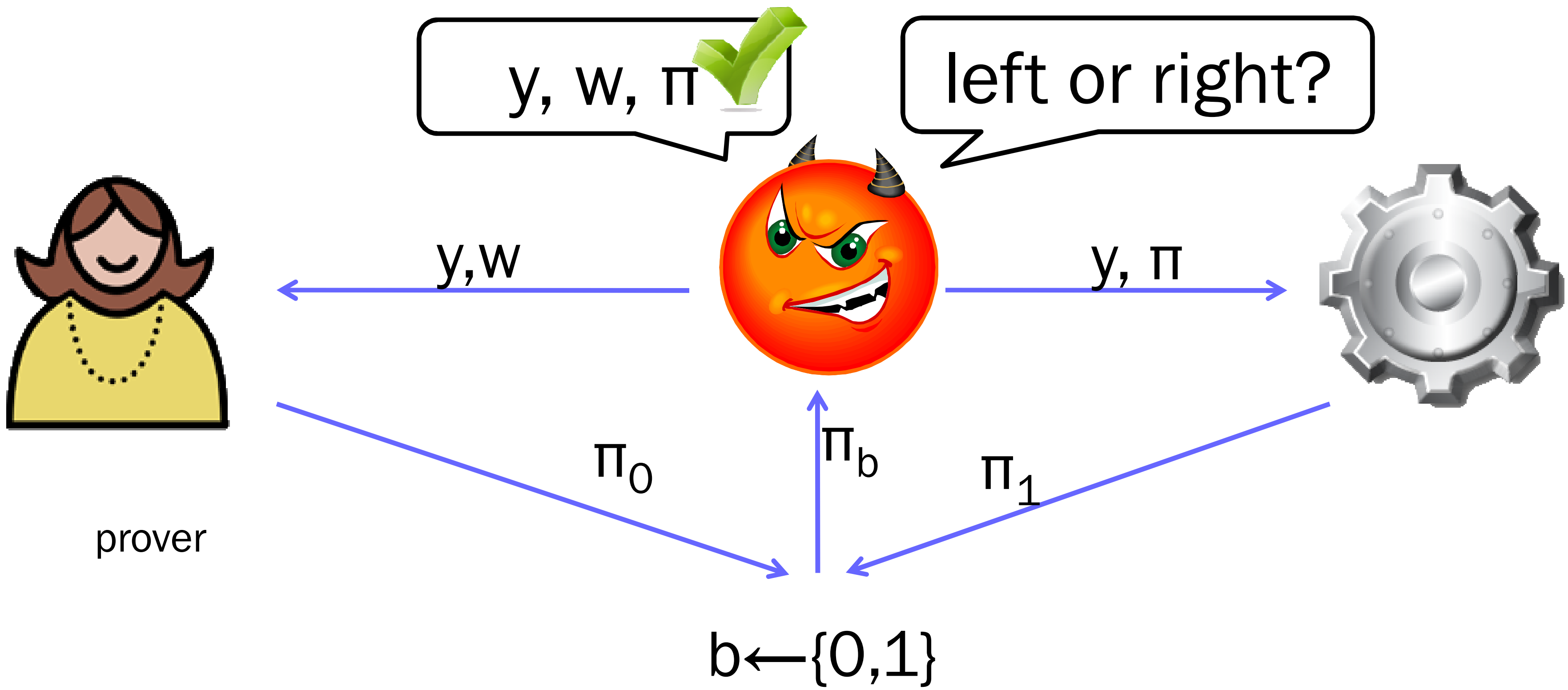
NymA = Com(skA)
NymB = Com(skB)
Cred = Com($\sigma_{skA}$(skB,attributes))

$\pi_1$: proof that nymA, NymB and Cred correct



# TECHNICAL DETAILS

# DEFINITION OF RANDOMIZABILITY




- proof $\pi_1$ looks like fresh proof for y

# INSTANTIATIONS?

- Cannot be realized using Fiat Shamir transform.
  - Hash function fixes challenge
  - $y=g^x$: $g^r$, $c=H(g^r)$, $s=cx+r$; check $g^s=g^r * y^c$
- In random committed (hidden) bit model [FLS, KP]
  - Use parts of CRS directly as commitments
  - Require trapdoor to open commitments?

# GROTH SAHAI PROOFS

- Homomorphic commitment scheme
  - $\mathrm{Com}(a, r_1) \cdot \mathrm{Com}(b, r_2) = \mathrm{Com}\,(a \cdot b, r_1 + r_2)$
- Bilinear map E in committed domain

- To prove $\prod_{q=1} e(x_q, y_q) = a$
  - for $x_q$, $y_q$ in $C_q$, $D_q$
  - compute pairing of commitments $\prod_{q=1} E(C_q, D_q) = A$

- Proof π shows that $A/\mathrm{Com}(a, 0)$ is commitment to 1

# RANDOMIZING GROTH SAHAI PROOFS

Randomize $(\{C_q, D_q\}, \pi)$

Old proof $\pi$ shows

(1) $A \,/\, \mathrm{Com}(a, 0) = \mathrm{Com}(1)$.

- Step 1: Randomize $C_q$, $D_q$ to $C'_q$, $D'_q$.
  - Multiply by random commitment to 1.
  - $\prod_{q=1..Q} E(C'_q, D'_q) = A'$
- Step 2: Compute $\pi_R$ that shows

  (2) $A' \,/\, A = \mathrm{Com}(1)$
- Step 3: Multiply proofs $\pi * \pi_R$ to show

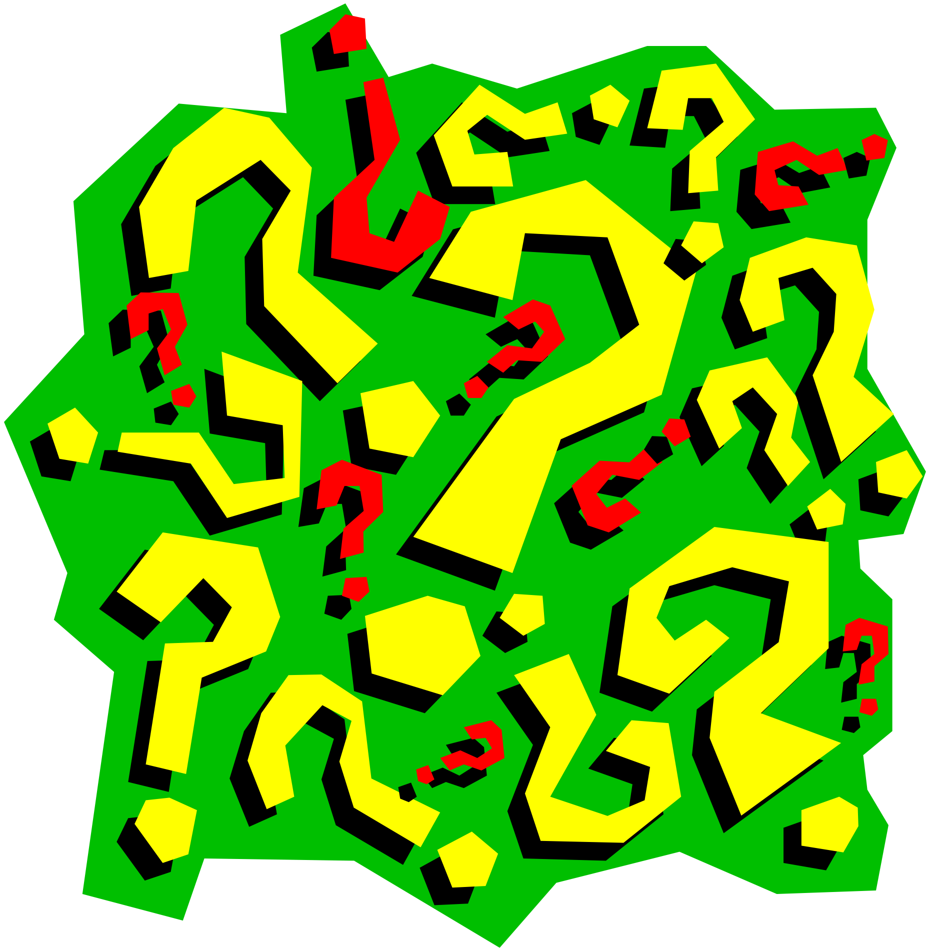
  (3) $A'/\mathrm{Com}(a,0) = \mathrm{Com}(1)\ \mathrm{Com}(1)$

# CONCLUSIONS

- Define randomizability
- Give randomizable NIZK proofs
  - for NP, building on [GOS]
  - leading to efficient applications building on [GS]

- Application: delegatable anonymous credentials
- Other applications? Other instantiations?

# QUESTIONS



# EXAMPLE FOR COMPOSITE ORDER GROUPS

- $g \in G$, $h \in G_q$ $E=e$
- Multiplication gate: $e(g^x, g^y) * e(g^z, g^{-1}) = 1$
  - $C_1 = g^x h^r$ , $C_2 = g^y h^s$ , $C_3 = g^{xy} h^t$
- $E(g^x h^r , g^y h^s) * E(g^{xy} h^t, g^{-1}) = E(h, g^{xs+yr-t} h^{rs})$
  - $\pi = g^{xs} g^{yr} g^{-t} h^{rs}$
- Randomize: $C_1$, $C_2$, $C_3$
  - $C'_1 = g^x h^{r+r'}$ , $C'_2 = g^y h^{s+s'}$ , $C'_3 = g^{xy} h^{t+t'}$
- $E(C'_1, C'_2) * E(C'_3, g^{-1}) = E(h, \pi) * E(g, C_1^{s'} C_2^{r'} g^{-t'} h^{r's'})$
  - $\pi' = C_1^{s'} C_2^{r'} g^{-t'} h^{r's'}$ and $\pi_R = \pi * \pi'$

# REFERENCES

(In order of appearance)


- [BDMP] Manuel Blum, Alfredo De Santis, Silvio Micali, Giuseppe Persiano: Noninteractive Zero-Knowledge. SIAM J. Comput. 20(6): 1084-1118 (1991)
- [FLS] Uriel Feige, Dror Lapidot, Adi Shamir: Multiple Non-Interactive Zero Knowledge Proofs Based on a Single Random String (Extended Abstract) FOCS 1990: 308-317
- [KP] Joe Kilian, Erez Petrank: Concurrent and resettable zero-knowledge in poly-logarithmic rounds. STOC 2001: 560-569
- [GOS] Jens Groth, Rafail Ostrovsky, Amit Sahai: Non-interactive Zaps and New Techniques for NIZK. CRYPTO 2006: 97-111 and
  Jens Groth, Rafail Ostrovsky, Amit Sahai: Perfect Non-interactive Zero Knowledge for NP. EUROCRYPT 2006: 339-358

# REFERENCES


- [GMR] Shafi Goldwasser, Silvio Micali, Charles Rackoff: The Knowledge Complexity of Interactive Proof Systems. SIAM J. Comput. 18(1): 186-208 (1989)
- [GS] Jens Groth, Amit Sahai: Efficient Non-interactive Proof Systems for Bilinear Groups. Electronic Colloquium on Computational Complexity (ECCC) 14(053): (2007)
- [DDN] Danny Dolev, Cynthia Dwork, Moni Naor: Nonmalleable Cryptography. SIAM J. Comput. 30(2): 391-437 (2000)
- [Sahai] Amit Sahai: Non-Malleable Non-Interactive Zero Knowledge and Adaptive Chosen-Ciphertext Security. FOCS 1999: 543-553
- [DDOPS] Alfredo De Santis, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano, Amit Sahai: Robust Non-interactive Zero Knowledge. CRYPTO 2001: 566-598

# REFERENCES


- [ElGamal] Taher El Gamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. CRYPTO 1984:10-18
- [Pallier] Pascal Paillier: Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. EUROCRYPT 1999:223-238
- [Gentry] Craig Gentry: Fully homomorphic encryption using ideal lattices. STOC 2009:169-178
- [PR] Manoj Prabhakaran, Mike Rosulek: Rerandomizable RCCA Encryption. CRYPTO 2007: 517-534
- [Groth] Jens Groth: Rerandomizable and Replayable Adaptive Chosen Ciphertext Attack Secure Cryptosystems. TCC 2004: 152-170
- [OO] Tatsuaki Okamoto, Kazuo Ohta: Divertible Zero Knowledge Interactive Proofs and Commutative Random Self-Reducibility. EUROCRYPT 1989:134-148

# REFERENCES


- [BDISS] Mike Burmester, Yvo Desmedt, Toshiya Itoh, Kouichi Sakurai, Hiroki Shizuya: Divertible and Subliminal-Free Zero-Knowledge Proofs for Languages. J. Cryptology (JOC) 12(3):197-223 (1999)
- [DY] Alfredo De Santis, Moti Yung: Cryptographic Applications of the Non-Interactive Metaproof and Many-Prover Systems. CRYPTO 1990:366-377
- [CLa] Melissa Chase, Anna Lysyanskaya: On Signatures of Knowledge. CRYPTO 2006:78-96
- [FP] Georg Fuchsbauer, David Pointcheval: Proofs on Encrypted Values in Bilinear Groups and an Application to Anonymity of Signatures. Pairing 2009:132-149
- [Chaum] David Chaum: Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Commun. ACM (CACM) 28(10):1030-1044 (1985)

# REFERENCES


- [Brands] Stefan Brands: Restrictive Blinding of Secret-Key Certificates. EUROCRYPT 1995:231-247
- [CLb] Jan Camenisch, Anna Lysyanskaya: An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. EUROCRYPT 2001:93-118