NON-INTERACTIVE RANDOMIZABLE PROOFS AND
DELEGATABLE ANONYMOUS CREDENTIALS

Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss,
Anna Lysyanskaya, and Hovav Shacham
NON-INTERACTIVE ZERO KNOWLEDGE PROOFS

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

Statement: \( y \in L \)

Witness \( w \) → Prover → Proof \( \pi \) → Verifier → yes/no

CRS
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**
  + Homomorphihic encryption [ElGamal, Paillier, Gentry]
  + RCCA encryption [PR, Groth]
  + Translation between pseudonyms:

\[ y_1 \text{ about Nym}_1 = \text{Com}(x, r_1), \quad y_2 \text{ about Nym}_2 = \text{Com}(x, r_2) \]

\[ y_1, \pi \rightarrow y_2, \pi' \rightarrow y_2, \pi'' \]

- **maul**
- **randomize**

- **proof** $\pi''$ looks like fresh proof for $y_2$
Credentials help manage large systems.

B will be forum admin.

C will be topic moderator.

Your credentials are good, I remove post.

I want this post removed.
DELEGATION OF CREDENTIALS

- Signatures $\rightarrow$ delegatable credentials

$\sigma_1, \sigma_2, \sigma = \text{Sign}_{sk_C}(m)$

$\sigma_1 = \text{Sign}_{sk_A}(pk_B)$

$\sigma_1, \sigma_2 = \text{Sign}_{sk_B}(pk_C)$
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
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 ANONYMOUS CREDENTIALS

- Use randomizable proofs

\[ \text{NymA} = \text{Com}(\text{skA}) \]
\[ \text{NymB} = \text{Com}(\text{skB}) \]
\[ \text{Cred} = \text{Com}(\sigma_{\text{skA}}(\text{skB})) \]

\( \pi_1 \): proof that NymA, NymB and Cred correct
DELEGATABLE ANONYMITY

Use randomizable proofs

maul & randomize

NymA = Com(skA), NymB' = Com(skB)
Cred' = Com(σ_{skA}(skB))
Proof π'₁: nymA, nymB' and Cred correct

NymC = Com(skC)
Cred = Com(σ_{skB}(skC))
Prove π₂: nymB', NymC and Cred correct

NymA = Com(skA)
NymB = Com(skB)
Cred = Com(σ_{skA}(skB))
π₁: proof that nymA, NymB and Cred correct

π'₁, π₂
Use randomizable proofs

\[ \text{NymA} = \text{Com}(\text{skA}), \quad \text{NymB} = \text{Com}(\text{skB}), \quad \text{Cred} = \text{Com}(\sigma_{\text{skA}}(\text{skB}, \text{attributes})) \]

\[ \pi_1: \text{proof that nymA, NymB and Cred correct} \]
TECHNICAL DETAILS
**DEFINITION OF RANDOMIZABILITY**

- $y, w, \pi$  
- left or right?

- $b \leftarrow \{0,1\}$

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

- Cannot be realized using Fiat Shamir transform.
  - Hash function fixes challenge
  - $y = g^x$, $c = H(g^r)$, $s = cx + r$; check $g^s = g^r \cdot y^c$

- 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
  + \( \text{Com}(a, r_1) \cdot \text{Com}(b, r_2) = \text{Com}(a \cdot b, r_1 + r_2) \)

- Bilinear map \( E \) in committed domain

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

- Proof \( \pi \) shows that \( A/\text{Com}(a, 0) \) is commitment to 1
Randomize (\{C_q, D_q\}, \pi)

Old proof \(\pi\) shows

\[(1) \quad A / \text{Com}(a, 0) = \text{Com}(1).\]

- **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

\[(2) \quad A' / A = \text{Com}(1)\]

- **Step 3:** Multiply proofs \(\pi \ast \pi_R\) to show

\[(3) \quad A'/\text{Com}(a,0) = \text{Com}(1) \text{ Com}(1)\]
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?
EXAMPLE FOR COMPOSITE ORDER GROUPS

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

(In order of appearance)

REFERENCES

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
REFERENCES


REFERENCES