GROTH-SAHAI PROOFS REVISITED

E. Ghadafi N.P. Smart B. Warinschi

Department of Computer Science,
University of Bristol

13th International Conference on Practice and Theory in Public Key Cryptography 2010

OUTLINE

OUTLINE

OUTLINE

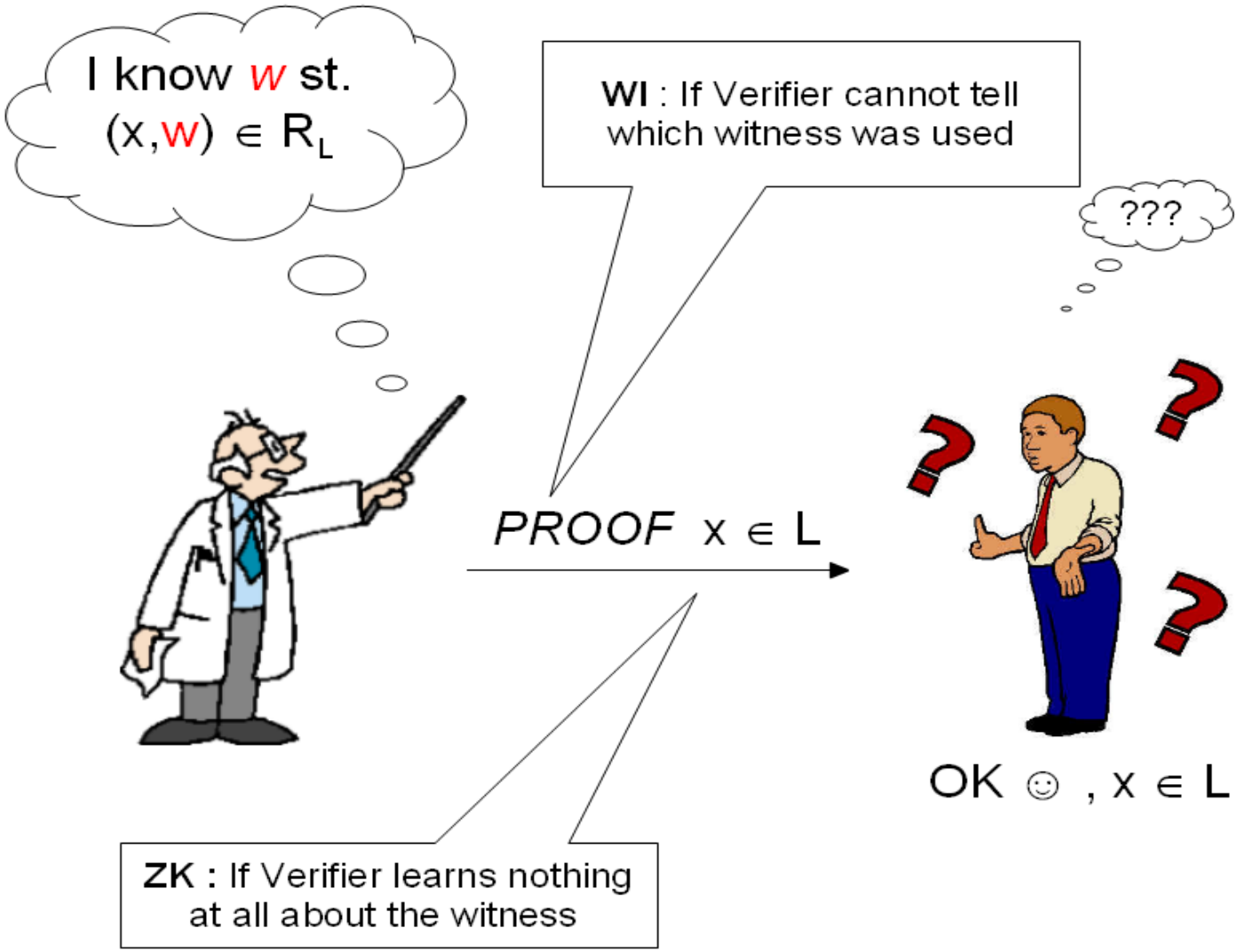
Outline

Outline

Outline

NON-INTERACTIVE PROOFS

"A proof is whatever convinces me.", Shimon Even.



PROPERTIES OF NIZK PROOFS

- **Completeness:**
  Verifier always accepts a valid proof.
- **Soundness:**
  Prover only has a negligible probability in making the verifier accept a proof for a false statement.
- **(Composable) Zero-Knowledge:**
  Verifier cannot tell a real proof from a simulated one.

APPLICATIONS OF ZERO-KNOWLEDGE PROOFS

Example applications:

- **Anonymous Credentials:** Client proves he possesses the required credentials without revealing them.
- **Online Voting:** Voter proves to the server that he has voted correctly without revealing his actual vote.
- **E-Cash, Signature Schemes, Oblivious Transfer , CCA-2 Encryption Schemes, ...**

HISTORY OF NIZK PROOFS

- Blum-Feldman-Micali, 1988.
- Damgard, 1992.
- Killian-Petrank, 1998.
- Feige-Lapidot-Shamir, 1999.
- De Santis-Di Crescenzo-Persiano, 2002.
- Groth-Sahai, 2008.

OUR CONTRIBUTION

- We present a correction to a minor problem in GS NIWI proofs under the DLIN and XSDH assumptions.

- We extend GS proofs to work under Type-2 pairings; the previous formulation only worked under Type-1 and Type-3 pairings.

BILINEAR GROUPS

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are finite cyclic groups of order n (prime or composite number), where $\mathbb{G}_1 =< P_1 >$ and $\mathbb{G}_2 =< P_2 >$.

Pairing $(e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T)$:
The function e must have the following properties:

- Bilinearity: $\forall Q_1 \in \mathbb{G}_1$, $Q_2 \in \mathbb{G}_2$ $x, y \in \mathbb{Z}_n$, we have

$$e([x]Q_1, [y]Q_2) = e(Q_1, Q_2)^{xy}.$$

- Non-Degeneracy: The value $e(P_1, P_2) \neq 1$ generates $\mathbb{G}_T$.
- The function e is efficiently computable.

PAIRINGS' TYPES

- **Type-1**:
  This is the symmetric pairing setting in which $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$ and $e : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T$.
- **Type-2**:
  $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$, where $\mathbb{G}_1 \neq \mathbb{G}_2$ and there is an efficiently computable isomorphism $\psi : \mathbb{G}_2 \longrightarrow \mathbb{G}_1$ where $\psi(P_2) = P_1$.
- **Type-3**:
  $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$, where $\mathbb{G}_1 \neq \mathbb{G}_2$, but there is no known efficiently computable isomorphism.

GROTH-SAHAI PROOFS

$$\mathbb{A}_1 \quad \times \quad \mathbb{A}_2 \quad \xrightarrow{f} \quad \mathbb{A}_T$$

GROTH-SAHAI PROOFS

$$\begin{array}{ccccc} \mathbb{A}_1 & \times & \mathbb{A}_2 & \xrightarrow{f} & \mathbb{A}_T \\ \iota_1 \downarrow\uparrow \rho_1 & & \iota_2 \downarrow\uparrow \rho_2 & & \iota_T \downarrow\uparrow \rho_T \\ \mathbb{B}_1 & \times & \mathbb{B}_2 & \xrightarrow{F} & \mathbb{B}_T \end{array}$$

GROTH-SAHAI PROOFS

$$\begin{array}{ccccc} \mathbb{A}_1 & \times & \mathbb{A}_2 & \xrightarrow{f} & \mathbb{A}_T \\ \iota_1 \downarrow\uparrow \rho_1 & & \iota_2 \downarrow\uparrow \rho_2 & & \iota_T \downarrow\uparrow \rho_T \\ \mathbb{B}_1 & \times & \mathbb{B}_2 & \xrightarrow{F} & \mathbb{B}_T \end{array}$$

Properties:

$$\forall x \in \mathbb{A}_1, \forall y \in \mathbb{A}_2 : F(\iota_1(x), \iota_2(y)) = \iota_T(f(x,y)),$$
$$\forall \mathcal{X} \in \mathbb{B}_1, \forall \mathcal{Y} \in \mathbb{B}_2 : f(p_1(\mathcal{X}), p_2(\mathcal{Y})) = p_T(F(\mathcal{X}, \mathcal{Y})).$$

How does it work?

Commit to the secrets(the witness), and just plug the commitments into the original equations you are proving!

Binding Setting $\Longrightarrow$ Perfect Soundness (Allows witness extraction).

Hiding Setting $\Longrightarrow$ Perfect Witness Indistinguishability (Allows simulation).

GROTH-SAHAI PROOFS

Key Idea:

Adversary cannot distinguish which setting we are working in.

From NIWI to NIZK proofs ?

In many cases (apart from a few Pairing Product Equations cases), it is easy to transform a NIWI proof into a NIZK proof. Just transform the equation into an equation with a trivial right-hand side and using the trapdoor information open a commitment to 1 to 0.

What statements can be proven ?

A variety of statements related to bilinear groups.

TYPES OF EQUATIONS

- Pairing Product Equation

$$\prod_{i=1}^{n1} e(A_i, Y_i) \cdot \prod_{i=1}^{n2} e(X_i, B_i) \cdot \prod_{i=1}^{n1}\prod_{j=1}^{n2} e(X_i, Y_j)^{r_{i,j}} = T$$

  here $T \in \mathbb{G}_T$
- Multi-scalar multiplication in $\mathbb{G}_1$

$$\sum_{i=1}^{n1} y_i A_i + \sum_{i=1}^{n2} b_i X_i + \sum_{i=1}^{n1}\sum_{i=j}^{n2} r_{i,j} y_j X_i = T_1$$

  here $T_1 \in \mathbb{G}_1$
- Multi-scalar multiplication in $\mathbb{G}_2$

$$\sum_{i=1}^{n1} a_i Y_i + \sum_{i=1}^{n2} x_i B_i + \sum_{i=1}^{n1}\sum_{i=j}^{n2} r_{i,j} x_i Y_j = T_2$$

  here $T_2 \in \mathbb{G}_2$
- Quadratic-equation in $\mathbb{Z}_p$

$$\sum_{i=1}^{n1} a_i y_i + \sum_{i=1}^{n2} x_i b_i + \sum_{i=1}^{n1}\sum_{i=j}^{n2} r_{i,j} x_i y_j = t$$

  here $t \in \mathbb{Z}_p$

HARD PROBLEMS

DEFINITION

Symmetric External Diffie-Hellman (SXDH) Assumption:

Setting : $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ (Type-3 Pairings)

Assumption: DDH problem is hard in both $\mathbb{G}_1$ and $\mathbb{G}_2$.

DEFINITION

Decisional Linear Problem(DLIN) Assumption:

Setting : $e : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T$ (Type-1 Pairings)

Input: $([a]P, [b]P, [ra]P, [sb]P, [t]P)$
where $a, b, r, s, t \in \mathbb{F}_q$

Assumption: It is hard to tell whether $t = r + s$ or t is random.

HARD PROBLEMS

DEFINITION

Symmetric Decisional Linear Problem(SDLIN) Assumption:

Setting : $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ (Type-2 and Type-3 Pairings)

Input: $([a_1]P_1, [b_1]P_1, [r_1a_1]P_1, [s_1b_1]P_1, [t_1]P_1)$
$([a_2]P_2, [b_2]P_2, [r_2a_2]P_2, [s_2b_2]P_2, [t_2]P_2)$
where $a_i, b_i, r_i, s_i, t_i \in \mathbb{F}_q$.

Assumption: It is hard to distinguish between the two situations:
$t_1 = r_1 + s_1$ and $t_2 = r_2 + s_2$
t_1 and t_2 are random.

CORRECTED GROTH-SAHAI NIWI PROOFS

$$\forall x \in \mathbb{A}_1, \forall y \in \mathbb{A}_2 : F(\iota_1(x), \iota_2(y)) = \iota_T(f(x,y))$$

Problem:

Under the XSDH and DLIN assumptions the original preprint version of the GS paper did not have functions for which the above commutative property held (for non-trivial values of $\iota_T(f(x,y))$)

How come no one spotted this before [65 papers] ???

CORRECTED GROTH-SAHAI NIWI PROOFS

$$\forall x \in \mathbb{A}_1, \forall y \in \mathbb{A}_2 : F(\iota_1(x), \iota_2(y)) = \iota_T(f(x,y))$$

Problem:

Under the XSDH and DLIN assumptions the original preprint version of the GS paper did not have functions for which the above commutative property held (for non-trivial values of $\iota_T(f(x,y))$)

How come no one spotted this before [65 papers] ???

- Proofs are usually used in a black-box way.
- NIZK proofs work fine.

CORRECTED GROTH-SAHAI NIWI PROOFS

$$\forall x \in \mathbb{A}_1, \forall y \in \mathbb{A}_2 : F(\iota_1(x), \iota_2(y)) = \iota_T(f(x,y))$$

Problem:

Under the XSDH and DLIN assumptions the original preprint version of the GS paper did not have functions for which the above commutative property held (for non-trivial values of $\iota_T(f(x,y))$)

How come no one spotted this before [65 papers] ???

- Proofs are usually used in a black-box way.
- NIZK proofs work fine.

Solution:

Modifying ι_T maps to ensure they have the required commutative properties will make the proofs work for any equation.

GS PROOFS UNDER THE SDLIN ASSUMPTION

We base the security of the proofs on the SDLIN assumption (i.e. requiring the DLIN holds in both $\mathbb{G}_1$ and $\mathbb{G}_2$).

Motivation:

- SXDH assumption only works in Type-3 pairings.
- DLIN assumption(as presented in GS) only works in Type-1 pairings.
- SDLIN assumption works in Type-1,2 and 3 pairings.

Efficiency:

We set $\mathbb{B}_1 = \mathbb{G}_1^3$, $\mathbb{B}_2 = \mathbb{G}_2^3$ and $\mathbb{B}_T = \mathbb{G}_T^9$, and we have:

$$F : \begin{cases} \mathbb{B}_1 \times \mathbb{B}_2 & \rightarrow & \mathbb{B}_T \\ (X_1, Y_1, Z_1), (X_2, Y_2, Z_2) & \mapsto & \begin{pmatrix} e(X_1, X_2) & e(X_1, Y_2) & e(X_1, Z_2) \\ e(Y_1, X_2) & e(Y_1, Y_2) & e(Y_1, Z_2) \\ e(Z_1, X_2) & e(Z_1, Y_2) & e(Z_1, Z_2) \end{pmatrix} \end{cases}$$

EVEN MORE EFFICIENT PROOFS IN TYPE-2 PAIRINGS

One can base the security of the proofs on both the DDH and DLIN assumptions at the same time(Highlighted to us by J. Groth).

How ?

Use DDH in $\mathbb{G}_1$ and DLIN in $\mathbb{G}_2$. This results more efficient proofs than using SDLIN.

Efficiency:

We set $\mathbb{B}_1 = \mathbb{G}_1^2$, $\mathbb{B}_2 = \mathbb{G}_2^3$ and $\mathbb{B}_T = \mathbb{G}_T^6$, and we have:

$$F : \begin{cases} \mathbb{B}_1 \times \mathbb{B}_2 & \longrightarrow & \mathbb{B}_T \\ (X_1, Y_1), (X_2, Y_2, Z_2) & \longmapsto & \begin{pmatrix} e(X_1, X_2) & e(X_1, Y_2) & e(X_1, Z_2) \\ e(Y_1, X_2) & e(Y_1, Y_2) & e(Y_1, Z_2) \end{pmatrix} \end{cases}$$

COMPARISON

Pairing Type	1	2	3	3
Hard Problems	DLIN	SDLIN	SDLIN	SXDH
$\lvert\mathbb{G}_1\rvert$ $\lvert\mathbb{G}_2\rvert$	1536/512 1536/512	256 3072	256 512	256 512
$\lvert\mathbb{B}_1\rvert$ $\lvert\mathbb{B}_2\rvert$	$3 \cdot \lvert\mathbb{G}_1\rvert = 4608/1536$ $3 \cdot \lvert\mathbb{G}_2\rvert = 4608/1536$	$3 \cdot \lvert\mathbb{G}_1\rvert = 768$ $3 \cdot \lvert\mathbb{G}_2\rvert = 9216$	$3 \cdot \lvert\mathbb{G}_1\rvert = 768$ $3 \cdot \lvert\mathbb{G}_2\rvert = 1536$	$2 \cdot \lvert\mathbb{G}_1\rvert = 512$ $2 \cdot \lvert\mathbb{G}_2\rvert = 1024$
Pairing Product Equations				
$(\hat{m}_1, \hat{m}_2)$ Size	(3,3) 13824/4608	(3,3) 29952	(3,3) 6912	(2,2) 3072
Multi-scalar multiplication in $\mathbb{G}_1$				
$(\hat{m}_1, \hat{m}_2)$ Size	(3,2) 13824/4608	(3,2) 29184	(3,2) 6144	(2,1) 2560
Multi-scalar multiplication in $\mathbb{G}_2$				
$(\hat{m}_1, \hat{m}_2)$ Size	(2,3) 13824/4608	(2,3) 20736	(2,3) 5376	(1,2) 2048
Quadratic Equations in $\mathbb{F}_q$				
$(\hat{m}_1, \hat{m}_2)$ Size	(2,2) 9216/3072	(2,2) 19968	(2,2) 4608	(1,1) 1536

TABLE: Summary of the different instantiations

SUMMARY

- NIWI proofs now verify for any equation.
- DLIN-Based NIZK and NIWI proofs that work in both Type-2 and Type-3 pairings.
- DLIN-Based proofs in Type-1 pairings can get more efficient due to the symmetry of F which does not hold in Type-2 and Type-3 pairings.
- Some people "prefer" DLIN because it is not as special as the SXDH and allows protocols to work in all 3 pairing types (Designers have to do their job only once !).
- Mixing DLIN and DDH assumptions results efficient NIWI and NIZK proofs in Type-2 and Type-3 Pairings.

The End

The End.
Questions?