Central European Conference on Cryptography

Trebic 2009

Protocols for graph isomorphism and hamiltonicity

Vadym Fedyukovych

New protocols were introduced for recognising directed graph isomorphism and directed graph hamiltonicity language membership, a novel challenge-response system, and a polynomial graph representation.

Protocols were developed by reducing problems to polynomials, replacing the witness with responses of Schnorr protocol, and by extending Schnorr protocol for testing properties of polynomials in challenge (of degree more than linear).

We achieve negligible soundness error in a single run, without repeating the protocol. Protocols are either of argument or of proof type, depending on commitment scheme used. Protocols are special honest verifier zero knowledge.

Polynomial complexity classes, NP, witness, NP-complete.

Graph isomorphism and hamiltonicity.

Commitment scheme, binding and hiding properties. Homomorphic property. Pedersen commitment scheme, unconditional hiding, computational binding.

Interactive proof system: completeness and soundness, negligible vs. non-negligible error probabilities. Private input tape of Prover with a solution, polynomial-time machines, arguments vs. proofs. Of knowledge. Witness indistinguishable and witness hiding. Zero knowledge, honest verifier zero knowledge, special honest verifier zero knowledge.

Upper bound on number of roots of a polynomial over a field, probability to choose a root at random.

Common input: group generator g of a prime order q, group element y.

Private input of Prover: $x \in \mathbb{F}_q$ such that $y = g^x$.

1. Prover chooses α at random, calculates and sends W_0:

$$\alpha \in_R \mathbb{F}_q, \qquad W_0 = g^\alpha \tag{1}$$

2. Verifier chooses and sends a challenge:

$$e \in_R \mathbb{F}_q \tag{2}$$

3. Prover produces and sends a response:

$$X = ex + \alpha \pmod{q} \tag{3}$$

4. Verifier accepts if

$$g^X y^{-e} \prod_{k=0}^{0} W_k^{-e^k} = 1 \tag{4}$$

Consider a directed graph $\mathbf{\Gamma} = (\mathbf{V}, \mathbf{E})$, vertices $v \in \mathbf{V}$ and arcs $a \in \mathbf{E}$, nonzero labels $\{b_v\}$ from finite field and flags $s_a \in \{0, 1\}$.

Definition 1. We say *graph characteristic polynomial* is a mapping

$$\mathbb{F}_q \times \mathbb{F}_q \times \mathbf{\Gamma} \longmapsto \mathbb{F}_q : \qquad f(x, y, \mathbf{\Gamma}) = \prod_{\overrightarrow{H(a)T(a)} \in \mathbf{E}} (1 + xb_{H(a)} + yb_{T(a)})$$

Lemma 1. *Directed graphs* $\mathbf{\Gamma}$ *and* $\mathbf{\Gamma}'$ *are isomorphic iif unique labels can be assigned to both graphs such that*

$$f(x, y, \mathbf{\Gamma}) = f(x, y, \mathbf{\Gamma}')$$

Lemma 2. *A directed graph with a prime* $n = |\mathbf{V}|$, $n|(q-1)$ *is a Hamiltonian cycle iif labels* $\{t^j\}$ *can be assigned for some non-zero* $t \in \mathbb{F}_q$ *such that*

$$f(x, y, \mathbf{\Gamma}) = \prod_{j=0}^{n} (1 + xt^j + yt^{j+1})$$

Consider responses of Schnorr protocol for challenge z

$$B_v(z) = zb_v + \alpha_v$$

in place of labels for characteristic polynomial.

Definition 2. We say *graph verification polynomial* is a mapping

$$(\mathbb{F}_q)^3 \times \mathbf{\Gamma} \longmapsto \mathbb{F}_q : \quad F(x, y, z, \mathbf{\Gamma}) = \prod_{\overrightarrow{H(a)T(a)} \in \mathbf{E}} (z + xB_{H(a)}(z) + yB_{T(a)}(z))$$

Lemma 3. *Graph characteristic polynomial is the top coefficient of graph verification polynomial:*

$$F(x, y, z, \mathbf{\Gamma}) = \sum_{k=0}^{m} z^k F_k(x, y, \mathbf{\Gamma}), \qquad F_m(x, y, \mathbf{\Gamma}) = f(x, y, \mathbf{\Gamma}), \qquad m = |\mathbf{E}|$$

Consider responses for arc flags s_a and for another challenge z':

$$S_a(z') = z's_a + \beta_a$$

Definition 3. We say *graph marking polynomial* is a mapping

$$(\mathbb{F}_q)^4 \times \mathbf{\Gamma} \mapsto \mathbb{F}_q : \; F'(x,y,z,z',\mathbf{\Gamma}) = \prod_{\overrightarrow{H(a)T(a)} \in \mathbf{E}} (z'z + S_a(z')(xB_{H(a)}(z) + yB_{T(a)}(z)$$

Lemma 4. *Graph verification polynomial of a subgraph marked with '1' flags is the top coefficient of graph marking polynomial.*

$$F'(x,y,z,z',\mathbf{\Gamma}) = \sum_{i=0}^{m} z'^i F'_i(x,y,z,\mathbf{\Gamma}), \qquad F'_m(x,y,z,\mathbf{\Gamma}) = F(x,y,z,\mathbf{\Gamma}')$$

Assign $s_a = 1$ for arcs of the Hamiltonian cycle and $s_a = 0$ for all other arcs.

Theorem: soundness error of isomorphism and hamiltonicity protocols with Pedersen commitments is $O(\frac{m}{q})$, on assumption of hardness of DLP in the group used.

Major point: given a Verifier accepted for a word not from the language, either his challenge happen to be a root, or he manage to solve an instance of DLP.

Protocols become proofs with commitment scheme of unconditional binding.

Theorem: simulator algorithms exist for isomorphism and hamiltonicity protocols with Pedersen commitments such that protocols are special honest verifier unconditional zero knowledge.

IACR preprint 2008/363 for details.

Thanks to

'Algebraic' protocols with 'large' challenges (resulting in small soundness error) due to Schnorr (1989) and Guillou-Quisquater (1988).

Prover responses that are linear polynomials due to Chaum-Evertse-VanDeGraaf (1987) and Beth (1988).

Polynomial set representation due to Minsky-Trachtenberg-Zippel (2001).

A homomorphic commitment scheme due to Pedersen (1991).

National University of Singapore for support while starting this research.

Contribution: new protocols for problems on graphs, a novel challenge-response system, a polynomial graph representation, soundness and zero knowledge theorems.

Related problems solved: a protocol to show that set difference is below a threshold; polynomial sequence representation and a protocol to show that K copies of a pattern sequence are in a host sequence (IACR 2008/357); a protocol for a codeword of Goppa code and an error below a threshold (IACR 2008/359).

Questions?

Vadym Fedyukovych, `http://vf.org.ua/`