The Fiat-Shamir Heuristic and the Random Oracle Model

Nils Löken
Paderborn University
29. Juni 2016

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Outline

1. Finding suitable hardness assumption
2. Proof protocol security under that assumption
3. Proof signature security in random oracle model, rely on procotol security

The RSA Assumption

Idea: computing e-th roots modulo a composite number N is hard

The RSA Assumption

Formally: given ppt algorithm $\mathrm{GenRSA}(1^n) \to (N, e, d)$ for $N = p \cdot q$, p, q n-bit primes, $e > 1$ with $\gcd(e, \phi(N)) = 1$, $e \cdot d = 1 \mod N$.

Game $\mathbf{RSA} - \mathbf{inv}_{\mathcal{A},\mathrm{GenRSA}}(n)$:

1. $(N, e, d) \leftarrow \mathrm{GenRSA}(1^n)$
2. $z \leftarrow \mathbb{Z}_N^*$
3. $x \leftarrow \mathcal{A}(N, e, z)$
4. output 1 if $x^e = z$, 0 otherwise

RSA assumption: for all ppt algos $\mathcal{A}$, there is a negligible function $\mu(\cdot)$ such that

$$\Pr[\mathbf{RSA} - \mathbf{inv}_{\mathcal{A},\mathrm{GenRSA}}(n) = 1] \leq \mu(n).$$

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Protocol Security — Informally

Idea: An identification protocol is secure if it is hard for an adversary to impersonate a prover, even after having observed many protocol executions between honest parties.
Introduce oracle $\mathrm{Trans}_{\mathrm{sk}} \to (R, f, y)$; models eavesdropping.
Game (informally):

- Impersonator receives public key pk and gets access to $\mathrm{Trans}_{\mathrm{sk}}$, sends R and to challenger
- Challenger replies with uniform challenge f
- Impersonator responds with y and wins game if $y^e = R \cdot \mathrm{pk}^f \mod N$

GQ-Ident Security under RSA Assumption

Idea: construct inverter $\mathcal{I}$ for RSA from impersonator $\mathcal{B}$ for GQ-Ident.

Inverter $\mathcal{I}(N, e, z)$:

1. $\mathrm{params} := (N, e), \mathrm{pk} := z$
2. run $\mathcal{B}(\mathrm{params}, \mathrm{pk})$
   - answer $\mathrm{Trans}_{\mathrm{sk}}$ queries by invoking simulator (special honest verifier zero knowledge)
   - reply to R^* with $f^* \leftarrow \mathbb{Z}_e$
   - receive transcript y^*
3. if (R^*, f^*, y^*) is accepting, rewind $\mathcal{B}$ to obtain transcript (R^*, f', y'), $f^* \neq f'$
4. apply extractor to transcripts to obtain x with $x^e = z$ (special soundness)
5. output x

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

GQ-Ident Security under RSA Assumption

Game $\mathbf{RSA-inv}_{\mathcal{A},\mathsf{GenRSA}}(n)$:

1. $(N, e, d) \leftarrow \mathsf{GenRSA}(1^n)$
2. $z \leftarrow \mathbb{Z}_N^*$
3. $x \leftarrow \mathcal{A}(N, e, z)$
4. output 1 if $x^e = z$, 0 otherwise

RSA assumption: for all ppt algos $\mathcal{A}$, there is a negligible function $\mu(\cdot)$ such that

$$\Pr[\mathbf{RSA-inv}_{\mathcal{A},\mathsf{GenRSA}}(n) = 1] \leq \mu(n).$$

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

GQ-Sig EUF-CMA in RO-Model under RSA Assumption

Idea: Use ppt forger $\mathcal{A}$ against GQ-Sig to construct ppt impersonator $\mathcal{B}$ against GQ-Ident.

Simplifying assumptions:

- $\mathcal{A}$ never repeats queries to H twice
- Given signature $(m, (f, y))$, $\mathcal{A}$ adversary does not query $H(y^e \cdot \mathrm{pk}^{-f} \mod N, m)$
- If $\mathcal{A}$ outputs $(m, (f, y))$, it has previously queried $H(y^e \cdot \mathrm{pk}^{-f} \mod N, m)$

GQ-Sig EUF-CMA in RO-Model under RSA Assumption

$q(n)$ polynomial upper bound on number of $\mathcal{A}$'s queries to H
Impersonator $\mathcal{B}(\mathrm{params}, \mathrm{pk})$ with $\mathrm{params} = (N, e), \mathrm{pk} = z$:

1. $j \leftarrow \{1, \ldots, q(n)\}$
2. run $\mathcal{A}(\mathrm{params}, \mathrm{pk})$, answer queries
   - $H(R_i, m_i)$: if $i = j$, output R_j and receive challenge f^*; else $f \leftarrow \mathbb{Z}_e$; give f or f^* to $\mathcal{A}$
   - $\mathrm{Sign}_{\mathrm{sk}}(m)$: query $\mathrm{Trans}_{\mathrm{sk}}$, receive (R, f, y), give $\sigma := (f, y)$ to $\mathcal{A}$
3. let $(m, \sigma = (f, y))$ be $\mathcal{A}$'s output; $R := y^e \cdot \mathrm{pk}^{-f} \mod N$
4. if $(R, m) = (R_j, m_j)$, output y; else abort

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Literature

- Katz, J., Lindell, Y. Introduction to modern cryptography, second edition. Chapman & Hall/CRC, 2015.