A New RSA-Based Signature Scheme

Sven Schäge, Jörg Schwenk

Horst Görtz Institute for IT-Security

Africacrypt 2010

RSA-Based Signature Schemes

- Naïve RSA signature scheme not secure under the standard definition of security – adaptive chosen message attacks [GMR99].

RSA-Based Signature Schemes

- Naïve RSA signature scheme not secure under the standard definition of security – adaptive chosen message attacks [GMR99].
- RSA assumption is weaker than popular Strong RSA (SRSA) assumption. In contrast to SRSA: adversary is not allowed to choose from an exponentially large set of solutions.

RSA-Based Signature Schemes

- Naïve RSA signature scheme not secure under the standard definition of security – adaptive chosen message attacks [GMR99].
- RSA assumption is weaker than popular Strong RSA (SRSA) assumption. In contrast to SRSA: adversary is not allowed to choose from an exponentially large set of solutions.
- Only recently, in CRYPTO'09, Hohenberger and Waters (HW) presented the first hash-and-sign signature scheme that is solely secure under the RSA assumption.

RSA-Based Signature Schemes

- Naïve RSA signature scheme not secure under the standard definition of security – adaptive chosen message attacks [GMR99].
- RSA assumption is weaker than popular Strong RSA (SRSA) assumption. In contrast to SRSA: adversary is not allowed to choose from an exponentially large set of solutions.
- Only recently, in CRYPTO'09, Hohenberger and Waters (HW) presented the first hash-and-sign signature scheme that is solely secure under the RSA assumption.
- In this work: alternative RSA-based signature scheme with additional properties that are useful in privacy preserving systems.

Observations

- A single HW signature can be interpreted as a combination of several Gennaro-Halevi-Rabin signatures. (Observation 1)

Observations

- A single HW signature can be interpreted as a combination of several Gennaro-Halevi-Rabin signatures. (Observation 1)
- The SRSA-based Camenisch-Lysyanskaya (CL) scheme has proven very useful in many privacy preserving systems. Popular examples: Direct Anonymous Attestation (DAA), compact E-Cash. (Observation 2)

Observations

- A single HW signature can be interpreted as a combination of several Gennaro-Halevi-Rabin signatures. (Observation 1)
- The SRSA-based Camenisch-Lysyanskaya (CL) scheme has proven very useful in many privacy preserving systems. Popular examples: Direct Anonymous Attestation (DAA), compact E-Cash. (Observation 2)
- Three useful properties of CL scheme:

Observations

- A single HW signature can be interpreted as a combination of several Gennaro-Halevi-Rabin signatures. (Observation 1)
- The SRSA-based Camenisch-Lysyanskaya (CL) scheme has proven very useful in many privacy preserving systems. Popular examples: Direct Anonymous Attestation (DAA), compact E-Cash. (Observation 2)
- Three useful properties of CL scheme:
  1. Signature scheme supports signing several message blocks.

Observations

- A single HW signature can be interpreted as a combination of several Gennaro-Halevi-Rabin signatures. (Observation 1)
- The SRSA-based Camenisch-Lysyanskaya (CL) scheme has proven very useful in many privacy preserving systems. Popular examples: Direct Anonymous Attestation (DAA), compact E-Cash. (Observation 2)
- Three useful properties of CL scheme:
  1. Signature scheme supports signing several message blocks.
  2. There exist efficient (NIZK) protocols (in the ROM) to sign commited values.

Observations

- A single HW signature can be interpreted as a combination of several Gennaro-Halevi-Rabin signatures. (Observation 1)
- The SRSA-based Camenisch-Lysyanskaya (CL) scheme has proven very useful in many privacy preserving systems. Popular examples: Direct Anonymous Attestation (DAA), compact E-Cash. (Observation 2)
- Three useful properties of CL scheme:
  1. Signature scheme supports signing several message blocks.
  2. There exist efficient (NIZK) protocols (in the ROM) to sign commited values.
  3. There exist efficient (NIZK) protocols (in the ROM) for proving knowledge of a signature without revealing it.

Idea and Construction

- Idea: Combine Observation 1 & Observation 2

Idea and Construction

- Idea: Combine Observation 1 & Observation 2
  - Construct signatures that can be interpreted as the combination of several CL signatures. Perhaps the decisive properties of the CL scheme can still be found in the new construction!

Idea and Construction

- Idea: Combine Observation 1 & Observation 2
  - Construct signatures that can be interpreted as the combination of several CL signatures. Perhaps the decisive properties of the CL scheme can still be found in the new construction!
- Technique:

Idea and Construction

- Idea: Combine Observation 1 & Observation 2
  - Construct signatures that can be interpreted as the combination of several CL signatures. Perhaps the decisive properties of the CL scheme can still be found in the new construction!
- Technique:
  - Starting point CL scheme: CL proof considers three types of forgery.

Idea and Construction

- Idea: Combine Observation 1 & Observation 2
  - Construct signatures that can be interpreted as the combination of several CL signatures. Perhaps the decisive properties of the CL scheme can still be found in the new construction!
- Technique:
  - Starting point CL scheme: CL proof considers three types of forgery.
  - Key observation: two of these forgeries already reduce security to the RSA assumption.

Idea and Construction

- Idea: Combine Observation 1 & Observation 2
  - Construct signatures that can be interpreted as the combination of several CL signatures. Perhaps the decisive properties of the CL scheme can still be found in the new construction!
- Technique:
  - Starting point CL scheme: CL proof considers three types of forgery.
  - Key observation: two of these forgeries already reduce security to the RSA assumption.
  - Remaining type of forgery can be dealt with using the new proving techniques of HW.

Idea and Construction

- Idea: Combine Observation 1 & Observation 2
  - Construct signatures that can be interpreted as the combination of several CL signatures. Perhaps the decisive properties of the CL scheme can still be found in the new construction!
- Technique:
  - Starting point CL scheme: CL proof considers three types of forgery.
  - Key observation: two of these forgeries already reduce security to the RSA assumption.
  - Remaining type of forgery can be dealt with using the new proving techniques of HW.
  - In particular: integrate that for a string X all prefixes of X are processed as well.

Idea and Construction

- Idea: Combine Observation 1 & Observation 2
  - Construct signatures that can be interpreted as the combination of several CL signatures. Perhaps the decisive properties of the CL scheme can still be found in the new construction!
- Technique:
  - Starting point CL scheme: CL proof considers three types of forgery.
  - Key observation: two of these forgeries already reduce security to the RSA assumption.
  - Remaining type of forgery can be dealt with using the new proving techniques of HW.
  - In particular: integrate that for a string X all prefixes of X are processed as well.
  - Modified scheme still allows to reduce the first two forgeries to the RSA assumption (although the proof is slightly more complicated).

Contribution: New Signature Scheme with Useful Properties for Anonymity Preserving Systems

- Advantages

- Disadvantages

Contribution: New Signature Scheme with Useful Properties for Anonymity Preserving Systems

- Advantages
  - New scheme supports signing several message blocks
- Disadvantages

Contribution: New Signature Scheme with Useful Properties for Anonymity Preserving Systems

- Advantages
  - New scheme supports signing several message blocks
  - New scheme allows to sign commited values

- Disadvantages

Contribution: New Signature Scheme with Useful Properties for Anonymity Preserving Systems

- Advantages
  - New scheme supports signing several message blocks
  - New scheme allows to sign commited values
  - Proof technique can be transferred to Cramer-Shoup, Fischlin and Zhou signature scheme $\Rightarrow$ Several new RSA-based signature schemes!
- Disadvantages

Contribution: New Signature Scheme with Useful Properties for Anonymity Preserving Systems

- Advantages
  - New scheme supports signing several message blocks
  - New scheme allows to sign commited values
  - Proof technique can be transferred to Cramer-Shoup, Fischlin and Zhou signature scheme $\Rightarrow$ Several new RSA-based signature schemes!
- Disadvantages
  - Signatures are larger than in HW (by just a single exponent)

Contribution: New Signature Scheme with Useful Properties for Anonymity Preserving Systems

- Advantages
  - New scheme supports signing several message blocks
  - New scheme allows to sign commited values
  - Proof technique can be transferred to Cramer-Shoup, Fischlin and Zhou signature scheme $\Rightarrow$ Several new RSA-based signature schemes!
- Disadvantages
  - Signatures are larger than in HW (by just a single exponent)
  - Signature generation and verification take more time

Contribution: New Signature Scheme with Useful Properties for Anonymity Preserving Systems

- Advantages
  - New scheme supports signing several message blocks
  - New scheme allows to sign commited values
  - Proof technique can be transferred to Cramer-Shoup, Fischlin and Zhou signature scheme $\Rightarrow$ Several new RSA-based signature schemes!
- Disadvantages
  - Signatures are larger than in HW (by just a single exponent)
  - Signature generation and verification take more time
  - Until now: No efficient (NIZK) protocols for proving knowledge of a signature without revealing it. – Future Work!

Related Work

- RSA-based signature schemes in the standard model

Related Work

- RSA-based signature schemes in the standard model
  - Tree-based signature schemes (Dwork-Noar CRYPTO'94 and more efficient Cramer-Damgard CRYPTO'96)

Related Work

- RSA-based signature schemes in the standard model
  - Tree-based signature schemes (Dwork-Noar CRYPTO'94 and more efficient Cramer-Damgard CRYPTO'96)
  - Stateful signature scheme (Hohenberger-Waters EC'09)

Related Work

- RSA-based signature schemes in the standard model
  - Tree-based signature schemes (Dwork-Noar CRYPTO’94 and more efficient Cramer-Damgard CRYPTO’96)
  - Stateful signature scheme (Hohenberger-Waters EC’09)
  - HW (CRYPTO’09)

Related Work

- RSA-based signature schemes in the standard model
  - Tree-based signature schemes (Dwork-Noar CRYPTO'94 and more efficient Cramer-Damgard CRYPTO'96)
  - Stateful signature scheme (Hohenberger-Waters EC'09)
  - HW (CRYPTO'09)
- RSA-like (i.e. SRSA-based) hash-and-sign signature schemes in the standard model

Related Work

- RSA-based signature schemes in the standard model
  - Tree-based signature schemes (Dwork-Noar CRYPTO'94 and more efficient Cramer-Damgard CRYPTO'96)
  - Stateful signature scheme (Hohenberger-Waters EC'09)
  - HW (CRYPTO'09)
- RSA-like (i.e. SRSA-based) hash-and-sign signature schemes in the standard model
  - Gennaro-Halevi-Rabin (EC'99)

Related Work

- RSA-based signature schemes in the standard model
  - Tree-based signature schemes (Dwork-Noar CRYPTO'94 and more efficient Cramer-Damgard CRYPTO'96)
  - Stateful signature scheme (Hohenberger-Waters EC'09)
  - HW (CRYPTO'09)
- RSA-like (i.e. SRSA-based) hash-and-sign signature schemes in the standard model
  - Gennaro-Halevi-Rabin (EC'99)
  - Cramer-Shoup (ACM Trans. Inf. Syst. Sec.'00)

Related Work

- RSA-based signature schemes in the standard model
  - Tree-based signature schemes (Dwork-Noar CRYPTO'94 and more efficient Cramer-Damgard CRYPTO'96)
  - Stateful signature scheme (Hohenberger-Waters EC'09)
  - HW (CRYPTO'09)
- RSA-like (i.e. SRSA-based) hash-and-sign signature schemes in the standard model
  - Gennaro-Halevi-Rabin (EC'99)
  - Cramer-Shoup (ACM Trans. Inf. Syst. Sec.'00)
  - Zhou (Chin. Journ. of Elec.'01), Camenisch-Lysyankaya (SCN'02), Fischlin (PKC'03),

Complexity Assumption

Definition (RSA assumption (RSA))

Given an RSA modulus $n = pq$, where p, q are sufficiently large primes, a prime $\alpha < \phi(n)$ with $\gcd(\alpha, \phi(n)) = 1$, and an element $u \in \mathbb{Z}_n^*$, we say that the $(t_{\mathsf{RSA}}, \epsilon_{\mathsf{RSA}})$-RSA assumption holds if for all t_{RSA}-time adversaries $\mathcal{A}$

$$\mathsf{Pr}\left[(x) \leftarrow \mathcal{A}(n, u, \alpha),\ x \in \mathbb{Z}_n^*,\ x^\alpha = u \bmod n\right] \leq \epsilon_{\mathsf{RSA}},$$

where the probability is over the random choices of u, n, α and the random coins of $\mathcal{A}$.

Prime Mapping Function $t(X)$

- Very similar to HW except that prime mapping function may not be compressive!

Prime Mapping Function $t(X)$

- Very similar to HW except that prime mapping function may not be compressive!
- Ingredients:

Prime Mapping Function $t(X)$

- Very similar to HW except that prime mapping function may not be compressive!
- Ingredients:
  - pseudo-random permutation $f_k : \{0,1\}^{l_X} \rightarrow \{0,1\}^{l_X}$ with key k.

Prime Mapping Function $t(X)$

- Very similar to HW except that prime mapping function may not be compressive!
- Ingredients:
  - pseudo-random permutation $f_k : \{0,1\}^{l_X} \rightarrow \{0,1\}^{l_X}$ with key k.
  - random value $s \in_R \{0,1\}^{l_X}$.

Prime Mapping Function $t(X)$

- Very similar to HW except that prime mapping function may not be compressive!
- Ingredients:
  - pseudo-random permutation $f_k : \{0,1\}^{l_X} \rightarrow \{0,1\}^{l_X}$ with key k.
  - random value $s \in_R \{0,1\}^{l_X}$.
- Prime mapping function t: $t(X) := \texttt{nextprime}(s \oplus f_k(X))$

Prime Mapping Function $t(X)$

- Very similar to HW except that prime mapping function may not be compressive!
- Ingredients:
  - pseudo-random permutation $f_k : \{0,1\}^{l_X} \to \{0,1\}^{l_X}$ with key k.
  - random value $s \in_R \{0,1\}^{l_X}$.
- Prime mapping function t: $t(X) := \texttt{nextprime}(s \oplus f_k(X))$
- Let $X \in \{0,1\}^{l_X}$ and define $X^{(i)} := 0^{l_X - i} x_1 \ldots x_i \in \{0,1\}^{l_X}$ for all $i \in [l_X]$. (Prefix of X that consists of the first i bits).

  For convenience: $T(X) := \prod_{i=1}^{l_X} t(X^{(i)})$

Prime Mapping Function $t(X)$

- Very similar to HW except that prime mapping function may not be compressive!
- Ingredients:
  - pseudo-random permutation $f_k : \{0,1\}^{l_X} \to \{0,1\}^{l_X}$ with key k.
  - random value $s \in_R \{0,1\}^{l_X}$.
- Prime mapping function t: $t(X) := \texttt{nextprime}(s \oplus f_k(X))$
- Let $X \in \{0,1\}^{l_X}$ and define $X^{(i)} := 0^{l_X - i} x_1 \dots x_i \in \{0,1\}^{l_X}$ for all $i \in [l_X]$. (Prefix of X that consists of the first i bits).

  For convenience: $T(X) := \prod_{i=1}^{l_X} t(X^{(i)})$
- Lemma[HW]: Given $q = q(\kappa)$ distinct input values, the probability that $t(X)$ collides is negligible.

A New RSA-Based Signature Scheme $\mathcal{S}$ (slightly simplified)

- ***Gen***(1^κ): computes a balanced and safe RSA modulus $n = pq$ and three random generators e, f, g of $\mathcal{QR}_n$. Additionally, it draws $k \in_R \mathcal{K}$ and $s \in_R \{0,1\}^{l_X}$. $PK = (n, e, f, g, k, s)$, $SK = (p, q)$.

A New RSA-Based Signature Scheme $\mathcal{S}$ (slightly simplified)

- ***Gen***(1^κ): computes a balanced and safe RSA modulus $n = pq$ and three random generators e, f, g of $\mathcal{QR}_n$. Additionally, it draws $k \in_R \mathcal{K}$ and $s \in_R \{0,1\}^{l_X}$. $PK = (n, e, f, g, k, s)$, $SK = (p, q)$.
- ***Sign***(SK, m): chooses $r \in_R \{0,1\}^{l_r}$ and $X \in_R \{0,1\}^{l_X}$:

$$z = (ef^m g^r)^{1/T(X)} \bmod n.$$

  The final signature is $\sigma = (z, X, r)$

A New RSA-Based Signature Scheme $\mathcal{S}$ (slightly simplified)

- ***Gen***(1^κ): computes a balanced and safe RSA modulus $n = pq$ and three random generators e, f, g of $\mathcal{QR}_n$. Additionally, it draws $k \in_R \mathcal{K}$ and $s \in_R \{0,1\}^{l_X}$. $PK = (n, e, f, g, k, s)$, $SK = (p, q)$.
- ***Sign***(SK, m): chooses $r \in_R \{0,1\}^{l_r}$ and $X \in_R \{0,1\}^{l_X}$:

  $$z = (ef^m g^r)^{1/T(X)} \bmod n.$$

  The final signature is $\sigma = (z, X, r)$
- ***Verify***(PK, m, σ): checks if it holds for (z, X, r) that

  $$z^{T(X)} \stackrel{?}{=} ef^m g^r \bmod n.$$

Security

Theorem

Assume the $(t_{\textit{RSA}}, \epsilon_{\textit{RSA}})$-RSA assumption holds. Then, $\mathcal{S}$ is (q, t, ϵ)-secure against adaptive chosen message attacks provided that

$$q = q_{\textit{RSA}}, \;\; t \approx t_{\textit{RSA}},$$
$$\epsilon \leq 9ql_X\epsilon_{\textit{RSA}}/2 + \textit{negl}(\kappa).$$

Signing Message Blocks

- ***Gen***(1^κ): is the same as in our main RSA scheme except that it now chooses $u+2$ generators $e, f_1, \ldots, f_u, g$ of $\mathcal{QR}_n$.
- ***Sign***$(SK, m_1, \ldots, m_u,)$: to sign a message the signer draws random values $r \in \{0,1\}^{l_r}$ and $X \in \{0,1\}^{l_X}$. Next, it computes

$$z = \left(e g^r \prod_{i=1}^{u} f_i^{m_i} \right)^{1/T(X)} \mod n.$$

  The final signature is $\sigma = (z, X, r)$
- ***Verify***$(PK, m_1, \ldots, m_u, \sigma)$: to verify a signature (z, X, r) the verifier checks whether

$$z^{T(X)} \stackrel{?}{=} e g^r \prod_{i=1}^{u} f_i^{m_i} \mod n.$$

Protocol for Signing Commited Values

- Interactive ZK protocol between signer s and user u.

Protocol for Signing Commited Values

- Interactive ZK protocol between signer s and user u.
- Very similar to protocol for CL.

Protocol for Signing Commited Values

- Interactive ZK protocol between signer s and user u.
- Very similar to protocol for CL.
- Idea: if u successfully proves knowledge of a commited value m, then s processes the corresponding commitment such that the result is a signature on m.

The End

Thank you for your attention. Any questions?