Signature from a New Subgroup Assumption

Victor K. Wei

Dep. of Information Engineering, Chinese Univ. of Hong Kong, Hong Kong
kwwei@ie.cuhk.edu.hk

November 26, 2005

Abstract. We present a new signature whose security is reducible to a new assumptions about subgroups, the *Computational Conjugate Subgroup Members (CCSM) Assumption*, in the random oracle model.

1 Introduction

Boneh, Goh, and Nissim [3] introduced a new trapdoor structure. Groth, Ostrovsy, and Sahai [10] presented an instantiation as follows: Find a GDH (Gap Diffie-Hellman) group $\mathbb{G}_1$ of prime order q. Find its subgroup $\mathbb{G}$ of order $N = q_1 q_2$ where N is the product of two primes q_1 and q_2 of roughly the same size. Necessarily $N|(q-1)$. The *Decisional Subgroup Membership Problem* is as follows: Given $\mathbb{G}_1$, $\mathbb{G}$, N as above and an element $h \in \mathbb{G}$ which has half-half probability of having order N or q_1, determine which is the case. The *Decisional Subgroup Membership Assumption* is that no PPT algorithm can solve the problem with probability non-negligible over half. For more details about various subgroup intractability assumptions and their applications, see [4, 6, 5, 3, 10, 1].

In this paper, we present a signature whose security is reducible to a new assumption about subgroups. The *Computational Conjugate Subgroup Members (CCSM) Problem* is as follows: Given $\mathbb{G}_1$, $\mathbb{G}$, N as above in the Decisional Subgroup Membership Problem, compute two elements h_1 and h_2 of $\mathbb{G}$ satisfying $\text{order}(h_1) = q_1$ and $\text{order}(h_2) = q_2$. The *Computational Conjugate Subgroup Members (CCSM) Assumption* is that no PPT algorithm can compute a random instance of the CCSM Problem with non-negligible probability.

Our signature is existentially unforgeable against adaptive-chosen-plaintext attackers provided the CCSM Assumption holds in the random oracle (RO) model.

We use textbook security model for signatures, specifically *existential unforgeability against adaptive-chosen-plaintext attackers*. See, for example, Goldreich [7, 8].

2 The signature construction

Let $N = q_1 q_1$ be the product of two primes q_1 and q_2. Let $\hat{\mathbf{e}} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ be a pairing. Note in a pairing, we have $\hat{\mathbf{e}}(g^a, h^b) = \hat{\mathbf{e}}(g, h)^{ab}$. Let $\mathbb{G} \subset \mathbb{G}_1$ be a GDH group of order N. Let $g, h_1, h_2 \in \mathbb{G}$, order$(g) = n$, order$(g_1) = q_1$, order$(g_2) = q_2$. Signer sk-pk pair is $((h_1, h_2), (\hat{\mathbf{e}}, g, N))$

Assume all discrete logarithm bases are faily generated. Let$\mathcal{H}$ be a full-domain cryptographically secure hash function. The identity element of $\mathbb{G}$ is denoted as 1. Our signature scheme is as follows:

Protocol Sign_{csm}: Randomly generate $s_0, r_0, r_1 \in Z_n^*$, compute $s_1 = -s_0^2$ and compute commitments

$$T_0 = g_0^{s_0}, \quad T_1 = h_1 g_1^{s_0}, \quad T_2 = h_2 g_2^{s_0}, \tag{1}$$

$$D_0 = g_0^{r_0}, \quad D_3 = [\hat{\mathbf{e}}(T_1, g_2)\hat{\mathbf{e}}(g_1, T_2)]^{r_0} \hat{\mathbf{e}}(g_1, g_2)^{r_1}, \quad D_4 = T_0^{r_1} g_0^{r_1} \tag{2}$$

Note

$$\hat{\mathbf{e}}(T_1, T_2)\hat{\mathbf{e}}(g, 1)^{-1} = [\hat{\mathbf{e}}(T_1, g_2)\hat{\mathbf{e}}(g_1, T_2)]^{s_0} \hat{\mathbf{e}}(g_1, g_2)^{s_1}, \quad 1 = T_0^{s_0} g_0^{s_1} \tag{3}$$

Compute the challenge

$$c = \mathcal{H}(M, T_0, T_1, T_2, D_0, D_3, D_4) \tag{4}$$

where M is the message. Compute responses

$$z_0 = r_0 - c s_0, \quad z_1 = r_1 - c s_1 \tag{5}$$

The signature is

$$\sigma = (T_0, T_1, T_2, c, z_0, z_1) \tag{6}$$

The signature verification algorith is **Protocol** Vf_{csm}: Given a signature of the format (6), parse then compute

$$D_3 = [\hat{\mathbf{e}}(T_1, g_2)\hat{\mathbf{e}}(g_1, T_2)]^{z_0} \hat{\mathbf{e}}(g_1, g_2)^{z_1} [\hat{\mathbf{e}}(T_1, T_2)\hat{\mathbf{e}}(g, 1)^{-1}]^c, \tag{7}$$

$$D_0 = g_0^{z_0} T_0^c, \quad D_4 = T_0^{z_0} g_0^{z_1} \tag{8}$$

Verify the received challenge c equals to that computed from Equation (4), and verify the following before outputting 1 (i.e. $\mathsf{verified}$):

$$T_0, T_1, T_2 \in \mathbb{G} \ \wedge \ \hat{\mathbf{e}}(T_0, g_1) \neq \hat{\mathbf{e}}(T_1, g_0) \ \wedge \ \hat{\mathbf{e}}(T_0, g_2) \neq \hat{\mathbf{e}}(T_2, g_0) \tag{9}$$

Reductinist security theorem

Theorem 1. *Signature* Sign_{csm} *is* existentially unforgeable against adaptive-chosen-plaintext attackers *provided the* Computational Conjugate Subgroup Members (CCSM) Assumption *holds in the random oracle (RO) model.*

Proof Sketch: The simulation of the Signing Oracle is by the special HVZK simulation in the RO model. Using rewind (forking) simulation, we extract a witness $(\hat{h}_1, \hat{h}_2, \hat{s}_0, \hat{s}_1)$ satisfying

$$T_0 = g_0^{\hat{s}_0}, \quad \hat{h}_1 = T_1 g_1^{-\hat{s}_0}, \quad \hat{h}_2 = T_2 g_2^{-s_0}, \quad 1 = T_0^{\hat{s}_0} g_0^{\hat{s}_1} \tag{10}$$

$$\hat{\mathbf{e}}(T_1, T_2)\hat{\mathbf{e}}(g, 1)^{-1} = [\hat{\mathbf{e}}(T_1, g_2)\hat{\mathbf{e}}(g_1, T_2)]^{\hat{s}_0}\hat{\mathbf{e}}(g_1, g_2)^{\hat{s}_1} \tag{11}$$

The last relation implies $\hat{\mathbf{e}}(\hat{h}_1, \hat{h}_2) = \hat{\mathbf{e}}(g, 1)^{-1}$, and $\hat{h}_1 = g^{\alpha}$, $\hat{h}_2 = g^{\beta}$ for some $\alpha, \beta \in Z_N^*$, $\alpha\beta = 0 \pmod N$. Then Relation (9) implies that $\alpha \neq 0, \beta \neq 0 \pmod N$. Therefore, α and β are the two prime factors of N and $(\hat{h}_1, \hat{h}_2)$ violates the CCSM Assumption. □

Remark: It has been shown that zero-knowledge cannot be achieved using the Fiat-Shamir paradigm [9, 2]. Therefore, our signature Sign_{csm} is not likely to have (plain) zero-knowledge. However, a proof in the RO model is better than no proof at all, and it is an open problem to construct signatures from the CCSM Assumptions without random oracles.

References

1. Ben Adida and Douglas Wikstrom. Obfuscated ciphertext mixing. Cryptology ePrint Archive, Report 2005/394, 2005. http://eprint.iacr.org/.
2. Boaz Barak, Yehuda Lindell, and Salil P. Vadhan. Lower bounds for non-black-box zero knowledge. In *FOCS 2003*, pages 384–393. IEEE Computer Soceity, 2003.
3. D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-DNF formulas on ciphertexts. In *TCC2005*, volume 3378 of *LNCS*, pages 325–341. Springer-Verlag, 2004.
4. K. Gjosteen. *Subgroup membership problems and public key cryptosystems.* Dr. ing. thesis, Norwegian University of Science and Technology, 2004.
5. K. Gjosteen. Homomorphic cryptosystems based on subgroup membership problems. In *Mycrypt 2005*, volume 3715 of *LNCS*, pages 314–327. Springer-Verlag, 2005.
6. K. Gjosteen. Symmetric subgroup membership problems. In *PKC 2005*, volume 3386 of *LNCS*, pages 104–119. Springer-Verlag, 2005.
7. O. Goldreich. *Foundations of Cryptography.* Cambridge Univesity Press, 2001.
8. O. Goldreich. *Foundations of Cryptography*, volume 2. Cambridge Univesity Press, 2005.
9. Shafi Goldwasser and Yael Tauman Kalai. On the (in)security of the Fiat-Shamir paradigm. In *FOCS 2003*, pages 102–. IEEE Computer Soceity, 2003.
10. Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero knowledge for NP. Cryptology ePrint Archive, Report 2005/290, 2005. http://eprint.iacr.org/.