A Note on Signature Transformation Attacks and Confirmer Signatures

Victor K. Wei

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

September 27, 2006

Abstract. Camenisch and Michels in Eurocrypt 2000 introduced the signature trnaformation attack on designated confirmer signatures (DCS). We apply this attack on Gentry, et al. Asiacrypt 2005's DCS, and then repair it. We also further optimize their confirmation and disavowal efficiencies.

1 The result

Chaum [4] introduced the DCS (Designated Confirmer Signature). The signature verification requires the interaction with a confirmer who was designated by the signer when the signature was created. The motivation was to split the power to sign and the power to confirm in order to mitigate the overpower of the signer. Several applications benefit from such a power splitting [4, 2].

T. Okamoto [7] gave a formal security model for DCS, and a polynomial equivalence reduction between DCS and public-key encryption. Camenisch and Michels [3] presented an upgraded DCS security model which included the *signature transformation attacker* who can query the confirmation oracle with adaptively designed signer public key which is not obtained by the given key generation protocol.

Goldwasser and Waisbard [6] and Gentry, et al. [5] presented DCS without random oracles. [5]'s DCS has $O(1)$-size and the state-of-the-art efficiency of costing 10 (resp. 41) exponentiations in confirm (resp. disavow).

Contributions We apply Camenisch and Michels [3]'s signature transformation attack on Gentry, et al. [5]'s DCS, and then repair it. We also further optimize their confirmation and disavowal efficiencies. In this brief note, we do not include the security model or other definitions of terminologies. Consult the original references for details [4, 7, 3, 6, 5].

Review: [5]'s DCS is $\sigma' = (\sigma^*, \phi, c)$,

$$\begin{aligned} \phi &= Commit(m,r) = g^m h^r \in QR_{n^2} \\ c &= \mathsf{Enc}(\mathsf{pk}_C, r) = (u_1, u_1, u_3, u_4) = (g_1^\rho, g_2^\rho, d_3^\rho g_0^r, (d_1 d_2^\alpha)^\rho) \in QR_{n^2}^4 \\ \sigma^* &= \mathsf{Sign}(\mathsf{sk}_S, (\phi, c, \mathsf{pk}_S)) \end{aligned}$$

where $\alpha = Hash(u_1,\ u_2,\ u_3)$. The commitment is Pedersen's commitment. The base $g_0 = n+1$ allows the confirmer to compute the *partial discrete logarithm* in the Paillier system, and thus decrypt r. Sign is any secure signature without random oracles, with signer private key sk_S. The confirmer public key pk_C consists of $d_1 = g_1^{x_1} g_2^{x_2}$, $d_2 = g_1^{y_1} g_2^{y_2}$, $d_3 = g_1^z$. Its private key is $\mathsf{sk}_C = (x_1,\ x_2,\ y_1,\ y_2,\ z)$.

The *signature transformation attack*: Generate the transformed signature using $c' = c$, $r' = r$, $m' = m+1$, $\phi' = \phi g$, and a new signature using attacker's knowledge of sk_S which is granted in the security model. The transformed DCS has the same validity/invalidity as the pre-transformation DCS. Interacting with the $CVerC$ oracle yields the validity/invalidity of the transformed DCS, and therefore the validity/invalidity of the original pre-transformation DCS.

Repair: Change α above to

$$\alpha = Hash(u_1, u_2, u_3, \phi, \mathsf{pk}_S, \mathsf{pk}_C, m)$$

When queried with anything other than the (DCS, pk_S, m) in gauntlet, the confirmation oracle will not yield any non-negligible advantage on the invisibility of the validity the DCS [3].

We note that [5]'s DCS remains secure in their own model. However, after the repair above, they can explicitly embellish their model to state that attacker-designed signer public keys not sampled from the model-given key generation protocol are allowed in the confirmation oracle inputs. We also optimize [5]'s four-move concurrent zero-knowledge confirmation/disavowal protocol below.

We omit the straightforward confirmation protocol $CZK\{r : \phi g^{-m} = h^r\}$. To disavow, prove either of the following:

$$\begin{gathered} CZK\{(x_1, x_2, y_1, y_2) : d_1 = g_1^{x_1} \ \wedge\ d_2 = g_1^{y_1} g_2^{y_2} \\ \wedge\ u_4 \neq g_1^{x_1+\alpha y_1} g_2^{x_1+\alpha y_2}\} \\ CZK\{(z, \bar{r}) : d_3 = g_1^z \ \wedge\ u_3 = u_1^z g_0^{\bar{r}} \ \wedge\ \phi g^{-m} \neq h^{\bar{r}}\} \end{gathered}$$

They are equivalent to, respectively,

$$CZK\{(x_1, x_2, y_1, y_2, s_0, s_1 = s_0x_1, s_2 = s_0y_1, s_3 = s_0x_2, s_4 = s_0y_2) : \\ d_1 = g_1^{x_1}g_2^{x_2} \ \wedge \ d_2 = g_1^{y_1}g_2^{y_2} \ \wedge \ T = u_4^{-s_0}g_1^{s_1+\alpha s_2}g_2^{s_3+\alpha s_4} \\ \wedge \ 1 = d_1^{s_0}g_1^{-s_1}g_2^{-s_3} \ \wedge \ 1 = d_2^{s_0}g_1^{-s_2}g_2^{-s_4}\} \text{ with } T \neq 1$$

$$CZK\{(z, \bar{r}, s_0, s_1 = s_0\bar{r}) : d_3 = g_1^z \ \wedge \ u_3 = u_1^z g_0^{\bar{r}} \ \wedge \ T = (\phi^{-1}g^m)^{s_0}g^{s_1} \\ \wedge \ T_4 = g_4^{s_0} \ \wedge \ 1 = T_4^{\bar{r}}g_4^{-s_1}\} \text{ with } T \neq 1$$

The confirmation costs 4 moves totalling 3 exponentiations. The disavow costs 4 moves totally at most 32 exponentiations. In comparison, [5]'s confirmation (resp. disavowal) costs 4 moves and 10 exponentiations (resp. 16 moves and 41 exponentiations).

Generalizations: Other DCS schemes employing encryption as a black-box building block, e.g. those in [6, 5] and others, also risk signature transformatin attacks possibly beyond their security models. Our results suggest they can open the black box slightly and add more parameters to the hash inputs or other *tag* [1] generating mechanisms.

Acknowledgements to Hong Kong Earmarked Grants 4232-03E and 4328-02E for sponsorship.

References

1. Masayuki Abe, Rosario Gennaro, Kaoru Kurosawa, and Victor Shoup. Tag-kem/dem: A new framework for hybrid encryption and a new analysis of kurosawa-desmedt kem. In *EUROCRYPT 2004*, pages 128–146, 2004.
2. N. Asokan, Victor Shoup, and Michael Waidner. Optimistic fair exchange of digital signatures. In *EUROCRYPT 1998*, pages 591–606, 1998.
3. J. Camenisch and M. Michels. Confirmer signature schemes secure against adaptive adversaries. In *Eurocrypt 2000*, pages 243–258. Springer-Verlag, 2000. LNCS No. 2729.
4. D. Chaum. Designated confirmer signatures. In *Eurocrypt'94*, pages 86–91. Springer-Verlag, 1994. LNCS No. 435.
5. Craig Gentry, David Molnar, and Zulfikar Ramzan. Efficient designated confirmer signatures without random oracles or general zero-knowledge proofs. In *ASIACRYPT 2005*, volume 3788 of *LNCS*, pages 662–681. Springer-Verlag, 2005.
6. Shafi Goldwasser and Erez Waisbard. Transformation of digital signature schemes into designated confirmer signature schemes. In *TCC 2004*, volume 2951 of *LNCS*, pages 77–100. Springer-Verlag, 2004.
7. T. Okamoto. Designated confirmer signatures and public-key encryption are equivalen. In *Proc. CRYPTO '94*, pages 61–74, 1994.