Analysis of VMSS Schemes for Group Key Transfer Protocol

Ching-Fang Hsu, Shan Wu

Analysis of VMSS schemes for group key transfer protocol

Ching-Fang Hsu[1]✉ Shan Wu[2]✉

[1](Computer School, Central China Normal University, Wuhan, 430079, China)
[2](Wuhan Technology and Business University, Wuhan, 430065, China)
cherryjingfang@gmail.com

Abstract. Known group key transfer protocols in group communications using classical secret sharing require that a t-degree interpolating polynomial be computed in order to encrypt and decrypt the secret group key. Secret sharing plays an important role in ensuring the group communications security. A verifiable multi-secret sharing (VMSS) scheme is a multi-secret sharing scheme with the verifiable property. Recently, Zhao et al. and Dehkordi et al. successively proposed two threshold VMSS schemes. Shortly, using the same verification mechanism, Dehkordi et al. presented another two VMSS schemes. In these schemes, authors claimed that the dealer was absolutely impossible to become a cheater. In this paper, we show that in both Zhao scheme and Dehkordi scheme, a dishonest dealer may distribute a fake share to a certain participant, and then that participant would subsequently never obtain the true secret. Indeed, verification mechanism should be improved in these schemes; and furthermore our results highlight that extra cautions still be exercised when constructing schemes in this direction.

Results

A verifiable multi-secret sharing (VMSS) scheme is a multi-secret sharing scheme with the verifiable property. Recently, Zhao et al. [3] and Dehkordi et al. [1] successively proposed two threshold VMSS schemes. Shortly, using the same verification mechanism, Dehkordi et al. presented another two VMSS schemes [2]. In these schemes, authors claimed that the dealer was absolutely impossible to become a cheater. In this paper, we show that in both Zhao scheme and Dehkordi scheme, a dishonest dealer may distribute a fake share to a certain participant, and then that participant would subsequently never obtain the true secret. Indeed, verification mechanism should be improved in these schemes; and furthermore our results highlight that extra cautions still be exercised when constructing schemes in this direction.

Cryptanalysis of Zhao scheme

In Zhao scheme [3], we assume that D is a dishonest dealer. Let M_w ($w \in \{1.2,...,n\}$) be a certain participant in M . The goal of D is to distribute a fake share to M_w and M_w will not detect this and, hence, M_w would subsequently never obtain the true secret. A more detailed description of the attack is as follows:

(1) As a preliminary step, D chooses an integer s_{n+1} from the interval $[2, N]$ and computes $I_{n+1} = R_0^{s_{n+1}} \bmod N$ such that $I_{n+1} \neq I_i$ for $i = 1.2,...,n$;

(2) After polynomial $h(x) \bmod Q$ is constructed, D computes $y_i = h(I_i) \bmod Q$ for $i = 1.2,...,n$, $i \neq w$ and specially computes $y_w = h(I_{n+1}) \bmod Q$ instead of $y_w = h(I_w) \bmod Q$. Afterwards, D publishs $(y_1, y_2, ..., y_n)$ or $(y_1, y_2, ..., y_n, h(1), h(2), ..., h(k-t))$;

(3) When any t participants include M_w want to recover the secrets $P_1, P_2, .., P_k$ (without loss of generality, suppose participants $\{M_i\}_{i=1}^t$), it is easy to see that anybody can verify I_i' is true or false but can not verify y_i is matched with I_i or not for $i = 1.2,...,t$. Therefore, after the verifications are done, M_w is unable to detect any discrepancy on y_w (actually, $y_w = h(I_{n+1}) \bmod Q$ is not matched with I_w);

(4) By using Lagrange interpolation polynomial, these t participants include M_w will uniquely obtain another polynomial $h(x)' \bmod Q$ but not $h(x) \bmod Q$, since the complete share distributed to M_w, that is (I_w, y_w), is not correctly paired. As a consequence, M_w would never obtain the secrets $P_1, P_2, .., P_k$.

Through the attack, the verification mechanism of Zhao scheme is completely compromised.

Cryptanalysis of Dehkordi scheme

Indeed, the attack of Dehkordi scheme [1] is the same as that of Zhao scheme. In Dehkordi scheme [1], we assume that D is a dishonest dealer. Let M_w ($w \in \{1.2,...,n\}$) be a certain participant in M . The goal of D is to distribute a fake share to M_w and M_w will not detect this and, hence, M_w would

subsequently never obtain the true secret. A more detailed description of the attack is as follows:

(1) As a preliminary step, D chooses an integer $s_{n+1} \in \mathbb{Z}_N$ and computes $f(r, s_{n+1})$ such that $f(r, s_{n+1}) \neq f(r, s_i)$ for $i = 1.2, ..., n$;

(2) After $\{r, G_i = g^{f(r,s_i)}\}_{i=1}^{n}$ is published and polynomial $h(x) \bmod q$ is constructed, D computes $y_i = h(f(r, s_i)) \bmod q$ for $i = 1.2, ..., n$, $i \neq w$ and specially computes $y_w = h(f(r, s_{n+1})) \bmod q$ instead of $y_w = h(f(r, s_w)) \bmod q$. Afterwards, D publishs $(y_1, y_2, ..., y_n)$ or $(h(1), h(2), ..., h(k-t), y_1, y_2, ..., y_n)$;

(3) When any t participants include M_w want to recover the secrets $P_1, P_2, .., P_k$ (without loss of generality, suppose participants $\{M_i\}_{i=1}^{t}$), it is easy to see that anybody can verify $f(r, s_i)$ is true or false but can not verify y_i is matched with $f(r, s_i)$ or not for $i = 1.2, ..., t$. Therefore, after the verifications are done, M_w is unable to detect any discrepancy on y_w (actually, $y_w = h(f(r, s_{n+1})) \bmod q$ is not matched with $f(r, s_w)$);

(4) By using Lagrange interpolation polynomial, these t participants include M_w will uniquely obtain another polynomial $h(x)' \bmod q$ but not $h(x) \bmod q$, since the complete share distributed to M_w, that is $(f(r, s_w), y_w)$, is not correctly paired. As a consequence, M_w would never obtain the secrets $P_1, P_2, .., P_k$.

Through this attack, the verification mechanism of Dehkordi scheme [1] is completely compromised. Furthermore, since the newer VMSS schemes proposed by Dehkordi et al. in [2] are based on the same verification mechanism, our attack equally applies to them.

Countermeasure

The main flaw in Zhao scheme and Dehkordi scheme is that there are no way for the participant to check whether I_i (or $f(r, s_i)$) chose by her/himself and y_i published by D are correctly paired or not. All participants can not be sure that y_i is matched with I_i (or $f(r, s_i)$) by only checking the correctness of I_i (or $f(r, s_i)$). This oversight allows the dishonest dealer in our attack to send the forged

y_i without being detected by the participant.

The simplest way to resolve the security problems with Zhao scheme and Dehkordi scheme would be to change the verification equations. For Dehkordi scheme, instead of computing $G_i = g^{f(r,s_i)}$ for $i = 1.2,...,n$, D need to compute $G_i = g^{P_{i+1}} \bmod p$ for $i = 0,1,2,...,k-1$ and publish them. Through checking $g^{y_i} = \prod_{j=0}^{t-1} (G_j)^{f(r,s_i)^j} \bmod p$ (if $k \le t$) or $g^{y_i} = \prod_{j=0}^{k-1} (G_j)^{f(r,s_i)^j} \bmod p$ (if $k > t$) for $i = 1.2,...,n$, the participants verify whether $f(r, s_i)$ and y_i are valid (i.e, correctly paired). After the secrets are recovered, the participants check $G_i = g^{P_{i+1}} \bmod p$ for $i = 0,1,2,...,k-1$ to verify whether $P_1, P_2, .., P_k$ are valid. As a consequence, our attack will no longer be valid against the fixed scheme. In the same way, this verification mechanism equally applies to Zhao scheme and the newer VMSS schemes proposed by Dehkordi et al. in [2].

Conclusion

This paper has considered the security of Zhao scheme and Dehkordi scheme for verifiable multi-secret sharing. Although these schemes claimed the dealer was absolutely impossible to become a cheater, we have shown that the schemes are indeed completely insecure against a dishonest dealer. In addition, we have recommended a small change to the schemes that can address the identified security problem. Furthermore, our attack and security patch apply also to the newer VMSS schemes proposed by Dehkordi et al.

References

[1] M. Hadian Dehkordi, S. Mashhadi, An efficient threshold verifiable multi-secret sharing, Computer Standards & Interfaces 30 (3) (2008) 187–190.

[2] M. Hadian Dehkordi, S. Mashhadi, New efficient and practical verifiable multi-secret sharing schemes, Information Sciences 178 (9) (2008) 2262–2274.

[3] J. Zhao, J. Zhang, R. Zhao, A practical verifiable multi-secret sharing scheme, Computer Standards & Interfaces 29 (1) (2007) 138–141.