

# A Note on Chosen-Basis Decisional Diffie-Hellman Assumptions

Michael Szydło

RSA Laboratories, Bedford, MA 01730.

`mszydlo@rsasecurity.com`

**Abstract.** This note discusses two Decisional Diffie-Hellman assumption variants introduced by Abdalla and Pointcheval at Financial Cryptography' 05. The authors introduce two new problems and assumptions: the Chosen-Basis Decisional Diffie-Hellman assumption #1 (CDDH1), and the Chosen-Basis Decisional Diffie-Hellman assumption #2 (CDDH2), and suggest that these assumptions warrant further analysis. The problems are each defined in terms of a formal experiment, and advantage function, and the assumption is that an adversary should have negligible advantage. However, in this note, we exhibit a simple adversary for each problem, such that the advantage is significant. These new assumptions were motivated by the requirements of a proof of security for a three party password authentication scheme described by the same authors. We conclude that the level of security assurance provided by this scheme is an open question.

**Key words:** chosen basis, Decisional Diffie-Hellman, interactive assumptions

## 1 Introduction

The Decisional Diffie-Hellman assumption is a well known cryptographic assumption. It is a simply stated, non-interactive assumption, and is often used as the basis of asymptotic and concrete security proofs. This note provides an analysis of two somewhat related assumptions introduced by Abdalla and Pointcheval at Financial Cryptography' 05[1]. The two new assumptions are more complex, and are defined with an interactive adversarial experiment, and corresponding advantage function. The authors conjectured that the new assumptions may be stronger than the usual Diffie-Hellman assumptions, and suggested that the new assumptions be studied further.

Our brief contribution is to provide an adversary for each such experiment which does have significant advantage. This shows that the assumptions themselves are not a sound basis for a security proof. These observations do not translate to a direct attack on the scheme, but only imply out that the existence of a proof of security is an open issue.

## 2 The CDDH1 Problem

The first new assumption is called the *Chosen-Basis Decisional Diffie-Hellman Assumption #1*. The new hard problem makes use of a cyclic group  $G$  of prime order  $p$ , generated by element  $g$ . This problem consists of an adversary running in two stages interacting in one of two games, specified by parameter  $b = 0$  or  $b = 1$ . The adversary's goal is to distinguish between the two games, i.e., the goal is determine whether  $b$  is 0 or 1. In the first stage the adversary is presented with three random elements of  $G$ ,  $U = g^u$ ,  $V = g^v$ , and  $X = g^x$ , where  $u, v, x$  are random elements in  $Z_p$ . The adversary can use these elements to generate an element  $Y$ . Next, a random bit  $b_0$  is generated, and  $b_1$  is set to  $b \oplus b_0$ . Based on  $b_0$  and  $b_1$ , and two random numbers  $r_0$  and  $r_1$ , two pairs of group elements  $(X_0, K_0)$ ;  $(X_1, K_1)$  and one group element  $Y_0$  are calculated as in Definition 1, below and presented to the adversary. The adversary must then output it's best guess at  $b$ .

The authors provide intuition suggesting that it would be difficult for an adversary to succeed with probability greater than  $1/2$ . This proceeds by evaluating two specific adversarial strategies. The first considers setting  $Y = g^y$  in the first stage, so that  $Y$  has known discrete log. The second considers setting  $Y = X/U$ . Indeed, it does appear that if the adversary follows these approaches, it will likely difficult to improve on randomly guessing  $b$  in the last stage. Before we present a better adversary, we recap the formal definition of the experiment from [1].

**Definition 1** *Let a  $G$  be a cyclic group of prime order  $p$ , generated by element  $g$ , and let  $A$  be an adversary. For any group elements  $U, V$ , and  $X$  in  $G$ , modular integers  $r_0$  and  $r_1$  in  $Z_p$ , and  $b \in \{0, 1\}$  an experiment is defined by:*

**Experiment**  $\text{Exp}_{G,b}^{cddh1}(A, U, V, X, r_0, r_1)$

$(Y, s) \xleftarrow{R} A(\text{find}, U, V, X)$   
 $b_0 \xleftarrow{R} \{0, 1\}; b_1 = b \oplus b_0$   
 $X_0 \leftarrow (X/U)^{r_{b_0}}; K_0 \leftarrow \text{CDH}(X/U, Y)^{r_{b_0}}$   
 $X_1 \leftarrow (X/V)^{r_{b_1}}; K_1 \leftarrow \text{CDH}(X/V, Y)^{r_{b_1}}$   
 $Y' \leftarrow Y^{r_0}$   
 $d \leftarrow A(\text{guess}, s, X_0, K_0, X_1, K_1, Y')$   
 return  $d$

The advantage of  $A$  with respect to  $(U, V, X, r_0, r_1)$  is defined to be

$$2Pr[\mathbf{Exp}_{G,b}^{cddh1}(A, U, V, X, r_0, r_1) = b] - 1.$$

The advantage function  $\mathbf{Adv}_{G,b}^{cddh1}(A)$  of the entire experiment is defined to be the expected advantage when  $U, V, X, r_0, r_1$  are chosen at random.

The CDDH1 assumption is that for a time bounded adversary  $A$ , the advantage  $\mathbf{Adv}_{G,b}^{cddh1}(A)$  should be very small. However, we now exhibit an adversary

which has advantage of approximately  $1/2$ . In the first stage, the adversary will select  $Y = V/U$ . Upon reception of  $X_0$ ,  $X_1$ , and  $Y'$ , the adversary will test whether  $X_0/X_1 = Y'$ . If this is true, the adversary will output 0, otherwise it will output 1.

We now analyze this adversary. Notice that condition  $X_0/X_1 = Y'$  holds exactly when  $(X/U)^{r_{b_0}}/(X/V)^{r_{b_1}} = (V/U)^{r_0}$ . When  $b_0 = b_1$ , this always holds. Otherwise equality can only hold upon a coincidence of two of  $X, U, V$  or of  $r_0$  and  $r_1$ . Such a coincidence will happen with probability less than  $1/2p$ . So if  $b = 0$ , the adversary will be correct about half of the time, and if  $b = 1$ , the adversary will be correct almost all of the time. In fact, the probability of success is greater than  $3/4 - 1/2p$ . This implies that the advantage is about  $2(3/4 - 1/2p) - 1 = 1/2 - 1/p$ .

$$\mathbf{Adv}_{G,b}^{cddh1}(A) \approx 1/2$$

Thus, this adversary effectively breaks the CDDH1 assumption.

### 3 The CDDH2 Problem

The second new assumption is called the *Chosen-Basis Decisional Diffie-Hellman Assumption #2*. This new assumption is somewhat simpler, and is also interactive. The problem resembles the previous one except that the adversary chooses  $X$ , and no values of  $K$  are computed. Before exhibiting our adversary, we recap the definition of the CDDH2 Experiment.

**Definition 2** Let a  $G$  be a cyclic group of prime order  $p$ , generated by element  $g$ , and let  $A$  be an adversary. For any group elements  $U$ , and  $V$  in  $G$ , modular integers  $r_0$  and  $r_1$  in  $Z_p$ , and  $b \in \{0, 1\}$  an experiment is defined by:

**Experiment**  $\mathbf{Exp}_{G,b}^{cddh2}(A, U, V, r_0, r_1)$

$$\begin{aligned} (X, Y, s) &\stackrel{R}{\leftarrow} A(\text{find}, U, V) \\ b_0 &\stackrel{R}{\leftarrow} \{0, 1\}; b_1 = b \oplus b_0 \\ X_0 &\leftarrow (X/U)^{r_{b_0}}; X_1 \leftarrow (X/V)^{r_{b_1}}; Y' \leftarrow Y^{r_0} \\ d &\leftarrow A(\text{guess}, s, X_0, X_1, Y') \\ &\text{return } d \end{aligned}$$

The advantage of  $A$  with respect to  $(U, V, r_0, r_1)$  is defined to be

$$2Pr[\mathbf{Exp}_{G,b}^{cddh2}(A, U, V, r_0, r_1) = b] - 1.$$

The advantage function  $\mathbf{Adv}_{G,b}^{cddh2}(A)$  of the entire experiment is defined to be the expected advantage when  $U, V, r_0, r_1$  are chosen at random.

The CDDH2 assumption is that for a time bounded adversary  $A$ , the advantage  $\mathbf{Adv}_{G,b}^{cddh2}(A)$  should be very small. However, we now exhibit an adversary

which has advantage of approximately  $1/p$ ! In the first stage, the adversary will select  $X = (UV)^{1/2}$ . This requires the extraction of a square root in  $G$ , for which an efficient algorithm is known.  $Y$  is selected arbitrarily. Upon reception of  $X_0$  and  $X_1$ , the adversary will test whether  $X_0X_1 = 1$ . If this is true, the adversary will output 0, otherwise it will output 1.

We now analyze this adversary. Notice that condition  $X_0X_1 = 1$  holds exactly when  $(U/V)^{r_{b_0}/2} = (U/V)^{r_{b_1}/2}$ . When  $b_0 = b_1$ , this always holds. Otherwise equality can only hold upon a coincidence  $U = V$ , or  $r_0 = r_1$ . Such a coincidence will also only happen with probability less than  $1/2p$ . So if  $b = 0$ , the adversary will always be correct, and if  $b = 1$ , the adversary will be correct almost all of the time. In fact, the probability of success is greater than  $1 - 1/2p$ . This implies that the advantage is about  $2(1 - 1/2p) - 1 = 1 - 1/p$ , just short of 1.

$$\mathbf{Adv}_{G,b}^{cddh1}(A) \approx 1$$

Thus, this adversary effectively breaks the CDDH2 assumption.

## 4 Conclusions

Due to the existence of the two of adversaries we exhibit, the two new assumptions introduced in [1] appear not to be useful variants of the classic Diffie Hellman assumptions as they stand. The application of these assumptions to the proof of security of a three party password protocol in [1], thus appears to automatically render that security proof flawed. It is still possible that their protocol has desirable security properties, but the search for a reduction proof with respect to reasonable assumptions is an open research issue.

In general, proofs based on non-interactive assumptions do appear to be more compelling, and finding appropriate non-interactive assumptions (with one-stage adversaries) on which to base the security proof can be a significant challenge. Finally, due to the difficulty of producing security proofs *post-facto*, it may be more practical to design cryptographic schemes with security proofs in mind.

## References

1. M. Abdalla, and D. Pointcheval *Interactive Diffie-Hellman Assumptions With Applications to Password-Based Authentication*. In Financial Cryptology'05, Springer-Verlag, 2005.