Convertible Authenticated Encryption Based on DLP

– **Signature generation:** For signing a message M for U_b, U_a first chooses $k \in_R Z_q$ and computes

$$r = g^k \bmod p, \tag{6}$$

$$w = y_b^{(k + x_a)} \bmod p, \tag{7}$$

$$s = k + x_a\, h(M, r, w) \bmod q, \tag{8}$$

$$c = F(r, s, w)^{-1} M \bmod p, \text{ where } F \text{ is also a one-way hash function.} \tag{9}$$

The authenticated ciphertext $\delta = (c, r, s)$ is then sent to U_b.

– **Message recovery and Verification:** Upon receiving δ, U_b first computes

$$w = (ry_a)^{xb} \bmod p, \tag{10}$$

and then recovers the message as

$$M = F(r, s, w)c \bmod p. \tag{11}$$

He further verifies the signature by checking if

$$g^s = ry_a^{h(M, r, w)} \bmod p. \tag{12}$$

If it holds, U_b accepts the signature.

– **Conversion:** When the case of a later dispute over repudiation occurs, U_b can reveal the converted signature $\Omega = (r, s, w)$ for M. Thus, anyone can verify the converted signature with the assistance of Eq. (12).