An Efficient Construction of Dual-Receiver Encryption

Youngtae Youn and Adam Smith

Research Goal

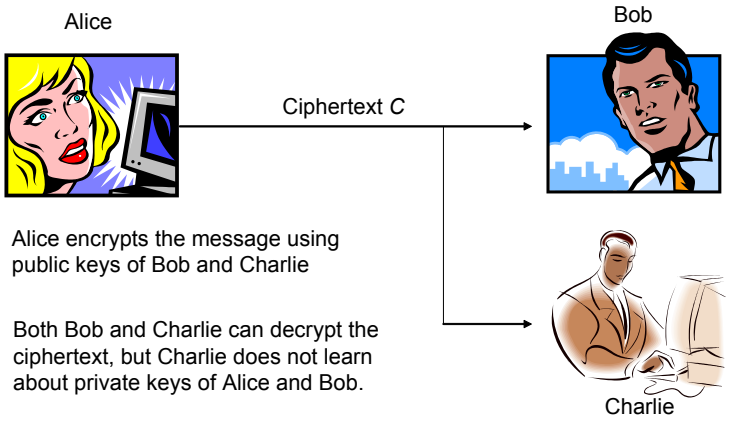
Dual Receiver Encryption (DRE) is a specialized encryption scheme.

- Anyone encrypts a plaintext to two receivers with a *single* ciphertext.
- It guarantees that both receivers will decrypt the *same* result.

DRE is a building block for other cryptographic primitives such as deniable authentication and key escrow.

General Idea: combine adaptively chosen ciphertext secure (CCA2-secure) encryption scheme and non-interactive zero-knowledge proof (NIZK)

- It results in prohibitively huge proof size.
- We devise an *efficient* construction based on bilinear maps in elliptic curves.



Deniable Authentication

DRE (Dual Receiver Encryption) is at the heart of Deniable Authentication.

- The receiver is *convinced* that the message originated from the sender.
- The receiver, even if malicious, *cannot* prove to anyone else that Charlie that the sender authenticated the given message.
- The receiver cannot be incriminated either, by a malicious sender.

Together with other building blocks such as NCE (Non-Committing Encryption), we can implement a deniable authentication protocol.

DRE can be also used to implement key escrow. [DLKY04]

[DLKY04] Diament et al, *The dual receiver cryptosystem and its applications,* ACM CCS 2004.

Building Blocks

$\mathrm{TBEgen}(1^k)$
$(p, \mathbb{G}, e, G_T) \xleftarrow{R} \mathcal{G}(1^k)$
$g \xleftarrow{R} G^*; i, j, k, l \xleftarrow{R} \mathbb{Z}_p^*$
Set $h, z \in G$ with $g^i = h^j = z$
$u \leftarrow g^k; v \leftarrow h^l$
$pk \leftarrow (\mathbb{G}, p, g, h, z, u, v)$
$sk \leftarrow (i, j)$
Return (pk, sk)

$\mathrm{TBEenc}(pk, t, M)$
$r, s \xleftarrow{R} \mathbb{Z}_p^*$
$V \leftarrow g^r; W \leftarrow h^s$
$X \leftarrow z^{ir} u^r; Y \leftarrow z^{js} v^s$
$K \leftarrow z^{r+s}$
$Z \leftarrow M \cdot K$
$C_{tbe} \leftarrow (V, W, X, Y, Z)$
Return C_{tbe}

$\mathrm{TBEdec}(sk, t, C_{tbe})$
$(V, W, X, Y, Z) \leftarrow C_{tbe}$
If C_{tbe} is valid then
$K \leftarrow V^i W^j$
Else $K \xleftarrow{R} G$
Return M

- Tag-based Encryption (TBE)
  - One way to achieve *CCA2-security* efficiently
- Groth-Sahai Proof System (GS Proof)
  - Enables NIZK proofs for *group-dependent* languages
- Assume that we have two ciphertexts C_i for (pk_i, sk_i) i=0,1

If there exist (r_0,s_0) and (r_1,s_1) such that the following equation holds, and C_1 are C_2 valid encryption of the same plaintext.

$$\frac{z_0^{r_0+s_0}}{z_1^{r_1+s_1}} = \frac{Z_0}{Z_1}, V_0 = g_0^{r_0}, W_0 = h_0^{s_0}, V_0 = g_1^{r_1}, W_1 = h_1^{s_1}$$

Construction

- Ciphertexts of Kiltz' Tag-based Encryption (TBE) consist of five group elements.
- If two ciphertexts contain the same plaintext, *five* linear equations on *eight* variables always hold.
- We construct Groth-Sahai (GS) Proof on these equations.
- The GS proof on these equations results with 34 group elements in bilinear group.
- The naïve approach use general NP-reduction to some NP languages such as *Circuit Satisfiability,* which ends up with thousands of gates – prohibitively expensive.
- In addition to space efficiency, this construction is also *provably secure* in the standard model.

Conclusion & Future Work

- Conclusion
  - *First* practical construction of Dual-Receiver Encryption
  - *Provably secure* in the standard model without resort to any heuristics such as random oracle model.
  - Useful building block: can be *applied* to many cryptographic protocols.
- Future works
  - Use other encryption schemes to *improve* performance.
  - Further *reduce* the size of NIZK proof.

Sponsored by the National Science Foundation