کشف شده باشد، می‌توان با اطمینان گفت که نتایج گسترده‌ی این فناوری جدید تا زمان مطالعه‌ی دیفی و هلمن، درک نشده بودند.

تمرین‌ها

۱۰-۱: فرض کنید Π یک پروتکل تبادل کلید و (Enc, Dec) یک طرح رمزگذاری کلید عمومی باشد. پروتکل «تعاملی» Π' زیر را برای رمزگذاری یک پیام در نظر بگیرید: در ابتدا، فرستنده و گیرنده، Π را اجرا می‌کنند تا یک کلید تسهیمی k را تولید کنند. سپس، فرستنده، $c \leftarrow Enc_k(m)$ را محاسبه کرده و c را برای طرف دیگر ارسال می‌کند که وی m را با استفاده از k رمزگشایی و بازیابی می‌کند.

(الف) تعریفی از رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر را فرمول‌بندی کنید (ن.ک. تعریف ۳-۸) که برای این موقعیت تعاملی، مناسب باشد.

(ب) اثبات کنید که اگر Π در حضور یک شنودگر، امن باشد و (Enc, Dec) دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر باشد، آنگاه Π' در تعریف شما صدق می‌کند.

۱۰-۲: نشان دهید که برای یکی از گروه‌های در نظر گرفته‌شده در بخش ۸-۳-۳ یا در بخش ۸-۳-۴، یک عنصر گروهی یکنواخت (نمایش داده‌شده با استفاده از نمایش طبیعی) به‌سادگی از یک رشته‌ی بیتی یکنواخت با طول یکسان، تمایزپذیر است.

۱۰-۳: یک حمله‌ی فرد در میانه علیه پروتکل دیفی-هلمن توصیف کنید که در آن، متخاصم یک کلید k_A را با آلیس و یک کلید (متفاوت) k_B را با باب تسهیم می‌کند و آلیس و باب نمی‌توانند تشخیص دهند که مشکلی پیش آمده است.

۱۰-۴: پروتکل تبادل کلید زیر را در نظر بگیرید:

(الف) آلیس، $k, r \in \{0,1\}^n$ یکنواخت را انتخاب کرده و $s := k \oplus r$ را برای باب ارسال می‌کند.

(ب) باب، $t \in \{0,1\}^n$ یکنواخت را انتخاب کرده و $u := s \oplus t$ را برای آلیس ارسال می‌کند.

(ج) آلیس، $w := u \oplus r$ را محاسبه کرده و w را برای باب ارسال می‌کند.

(د) آلیس، k را به‌عنوان خروجی ارائه می‌کند و باب، $w \oplus t$ را به‌عنوان خروجی ارائه می‌کند.

نشان دهید که آلیس و باب، کلید یکسانی را به‌عنوان خروجی ارائه می‌کنند. امنیت این طرح را تحلیل کنید (یعنی، یا امنیت آن را اثبات کنید یا یک حمله‌ی عینی را نشان دهید).

فصل یازدهم: رمزگذاری کلید عمومی

۱۱-۱- مروری بر رمزگذاری کلید عمومی

معرفی رمزگذاری کلید عمومی نشانگر انقلابی در رمزنگاری بود. تا آن زمان، رمزنگاران برای رسیدن به ارتباط خصوصی، به‌صورت اختصاصی به کلیدهای محرمانه‌ی تسهیم شده، تکیه می‌کردند. در مقابل، روش‌های کلید عمومی به طرفین اجازه می‌دهند که به‌صورت خصوصی ارتباط برقرار کنند بدون اینکه مجبور باشند از قبل بر روی هیچ اطلاعات رمزی توافق نمایند. همان‌طور که قبلاً اشاره کردیم، امکان‌پذیر بودن این امر بسیار شگفت‌آور بوده و برخلاف روال طبیعی است: این امر به این معنا است که دو نفر در دو طرف یک اتاق که تنها می‌توانند از طریق فریاد زدن باهم ارتباط برقرار کنند و هیچ رمز اولیه‌ای ندارند می‌توانند به صورتی صحبت کنند که هیچ شخص دیگری در اتاق هیچ‌چیزی در مورد آنچه می‌گویند نفهمد!

در موقعیت رمزگذاری کلید خصوصی، دو طرف بر یک کلید رمز توافق می‌کنند که می‌تواند توسط هر یک از طرفین برای رمزگذاری و رمزگشایی مورد استفاده قرار گیرد. رمزگذاری کلید عمومی از هر دو این جهات، «نامتقارن» است. یکی از طرفین (گیرنده) یک «زوج» کلید (pk, sk)، که به ترتیب کلید عمومی و کلید خصوصی نامیده می‌شوند، را تولید می‌کند. کلید عمومی توسط یک فرستنده برای رمزگذاری یک پیام استفاده می‌شود؛ گیرنده از کلید خصوصی برای رمزگشایی متن رمز به‌دست‌آمده، استفاده می‌کند.

ازآنجاکه هدف عبارت است از اجتناب از نیاز دو طرف برای ملاقات از قبل به‌منظور توافق بر روی اطلاعات، فرستنده چطور pk را می‌فهمد؟ روی مجرد، دو طریق برای رخداد این امر وجود دارد. گیرنده را آلیس و فرستنده را باب می‌نامیم. در رویکرد اول، هنگامی‌که آلیس می‌فهمد که باب می‌خواهد با وی ارتباط برقرار کند، می‌تواند در آن نقطه، (pk, sk) را تولید کند (با این فرض که این کار را قبلاً انجام نداده است) و سپس pk را برای باب «به‌صورت عیان» ارسال کند؛ سپس، باب می‌تواند از pk برای رمزگذاری پیام خود استفاده کند. تأکید می‌کنیم که کانال بین آلیس و باب

ممکن است عمومی باشد، ولی فرض بر آن است که این کانال، احراز اصالت شده است به این معنی که متخاصم نمی‌تواند کلید عمومی ارسال‌شده توسط آلیس برای باب را تغییر دهد (و علی‌الخصوص نمی‌تواند آن را با کلید خود، جایگزین کند). برای بحثی در خصوص چگونگی توزیع کلیدهای عمومی بر روی کانال‌های احراز اصالت نشده، به بخش ۱۲-۷ مراجعه کنید.

یک رویکرد دیگر آن است که آلیس کلیدهای خود (pk, sk) را از قبل و به‌صورت مستقل از فرستنده‌ای خاص، تولید کند. (درواقع، در زمان تولید کلید، نیازی نیست که آلیس اطلاع داشته باشد که باب می‌خواهد با وی صحبت کند یا حتی اینکه باب وجود دارد.) آلیس می‌تواند کلید عمومی خود یعنی pk را به‌صورت گسترده مثلاً با انتشار آن بر روی وب‌سایت خود، قرار دادن آن بر روی کارت ویزیت یا قرار دادن آن در یک فهرست عمومی، پخش کند. اکنون، هرشخصی که بخواهد به‌صورت خصوصی با آلیس ارتباط برقرار کند می‌تواند کلید عمومی وی را یافته و به‌مانند بالا عمل کند. توجه کنید که چندین فرستنده می‌توانند چندین بار با آلیس با استفاده از همان کلید عمومی pk برای رمزگذاری تمام ارتباطات خود، ارتباط برقرار کنند.

توجه کنید که در هرکدام از سناریوهای بالا، pk ذاتاً عمومی است–و بنابراین می‌تواند به‌سادگی توسط مهاجم، یافت شود. در حالت اول، متخاصم شنودگر بر ارتباط بین آلیس و باب، pk را به‌صورت مستقیم به دست می‌آورد. در حالت دوم، متخاصم می‌تواند کلید عمومی آلیس را خودش بیابد. مشاهده می‌کنیم که امنیت رمزگذاری کلید عمومی نمی‌تواند بر محرمانگی pk تکیه داشته باشد بلکه باید به محرمانگی sk تکیه کند. بنابراین، ضروری است که آلیس، کلید خصوصی خود را برای هیچ‌فردی فاش نکند، که شامل باب فرستنده هم می‌شود.

مقایسه با رمزگذاری کلید خصوصی

شاید واضح‌ترین تفاوت بین رمزگذاری کلید خصوصی و عمومی این است که اولی، «محرمانگی کامل» تمامی کلیدهای رمزنگاری را فرض می‌کند درحالی‌که دومی تنها برای کلید خصوصی sk، محرمانگی را ملزم می‌کند. هرچند این امر ممکن است یک تفاوت جزئی به نظر آید، نتایج آن بسیار عظیم هستند: در موقعیت کلید خصوصی، طرفین در حال ارتباط باید به‌گونه‌ای قادر به تسهیم یک کلید رمز بدون اجازه دادن به طرفین ثالث برای فهمیدن آن، باشند درحالی‌که در موقعیت کلید عمومی، کلید عمومی را می‌توان از یک طرف به طرف دیگر بر روی یک کانال عمومی ارسال نمود بدون اینکه خدشه‌ای به امنیت وارد شود. برای طرفینی که با فریاد از دو سوی یک اتاق صحبت می‌کنند یا در حالت واقع‌بینانه‌تر بر روی یک شبکه‌ی عمومی از قبیل خط تلفن یا اینترنت ارتباط برقرار می‌کنند، رمزگذاری کلید عمومی، تنها گزینه‌ی در دسترس است.

یک تفاوت مهم دیگر آن است که طرح‌های رمزگذاری کلید خصوصی از کلیدی یکسان برای رمزگذاری و رمزگشایی استفاده می‌کنند، درحالی‌که طرح‌های رمزگذاری کلید عمومی از کلیدهای

متفاوت برای هرکدام از این دو عملیات استفاده می‌کنند. یعنی، رمزگذاری کلید عمومی به شکل ذاتی، «نامتقارن» است. این عدم تقارن در موقعیت کلید عمومی به این معنا است که نقش‌های فرستنده و گیرنده قابل جابه‌جایی به‌مانند حالت کلید خصوصی نیستند: یک زوج کلید یکتا اجازه‌ی برقراری ارتباط تنها در یک‌جهت را می‌دهد. (ارتباط دو جهتی را می‌توان به چند طریق به دست آورد؛ نکته آن است که یک فراخوانی یکتا از یک طرح رمزگذاری کلید عمومی باعث ایجاد تمایز بین یک کاربر که به‌عنوان گیرنده عمل می‌کند و دیگر کاربران که به‌عنوان فرستنده عمل می‌کنند، خواهد شد.) به‌علاوه، یک نمونه‌ی یکتا از یک طرح رمزگذاری کلید عمومی به چندین فرستنده اجازه می‌دهد که به‌صورت خصوصی با یک گیرنده‌ی یکتا ارتباط برقرار کنند برخلاف حالت کلید خصوصی که در آن، یک کلید رمز تسهیم شده بین دو طرف، اجازه‌ی ارتباط خصوصی تنها بین همان دو طرف را می‌دهد.

با خلاصه کردن و تبیین بحث قبلی، مشاهده می‌کنیم که رمزگذاری کلید عمومی دارای مزیت‌های زیر نسبت به رمزگذاری کلید خصوصی است:

- رمزگذاری کلید عمومی، «مشکل توزیع کلید» را (تا حدودی(حل می‌کند چراکه نیازی نیست طرفین ارتباط، قبل از ارتباط خود، یک کلید را به شکل محرمانه تسهیم کنند. دو طرف می‌توانند ارتباط محرمانه داشته باشند حتی اگر کل ارتباط بین آن‌ها تحت نظر باشد.
- هنگامی‌که یک گیرنده‌ی یکتا در حال ارتباط با N فرستنده است (برای مثال، یک فروشنده‌ی آنلاین که سفارش‌های کارت اعتباری را از چندین خریدار، پردازش می‌کند)، برای گیرنده بسیار راحت‌تر است که یک کلید خصوصی یکتای sk را ذخیره کند تا اینکه N کلید رمز متفاوت (یعنی یک کلید برای هر فرستنده) را تسهیم، ذخیره و مدیریت نماید. درواقع، هنگام استفاده از رمزگذاری کلید عمومی، نیازی نیست که تعداد و هویت فرستندگان بالقوه در زمان تولید کلید، مشخص باشد. این امر اجازه‌ی انعطاف‌پذیری بسیار بالایی در «سیستم‌های باز» می‌دهد.

زمانی که یک گیرنده تنها می‌خواهد پیام‌هایی را از یک فرد خاص دریافت کند، این واقعیت که طرح‌های رمزگذاری کلید عمومی به همه اجازه می‌دهند تا به‌عنوان یک فرستنده عمل کنند می‌تواند یک نقطه‌ضعف باشد. در این حالت، یک طرح رمزگذاری (کلید خصوصی) احراز اصالت شده، یک انتخاب بهتر نسبت به رمزگذاری کلید عمومی خواهد بود.

اصلی‌ترین عیب رمزگذاری کلید عمومی آن است که تقریباً دو تا سه برابر کندتر از رمزگذاری کلید خصوصی است[۲۱]. پیاده‌سازی رمزگذاری کلید عمومی در دستگاه‌های دارای محدودیت شدید منابع از

---

[۲۱] ارائه‌ی یک مقایسه‌ی دقیق، دشوار است به این دلیل که کارایی نسبی به طرح‌های دقیق مدنظر و همین‌طور جزئیات مختلف پیاده‌سازی، بستگی دارد.

قبیل کارت‌های هوشمند یا برچسب‌های شناسایی فرکانس رادیویی (*RFID*) می‌تواند یک چالش باشد. حتی زمانی که یک رایانه‌ی رومیزی در حال اجرای عملیات رمزنگاری است، اجرای هزاران عملیات در ثانیه (مثل حالتی که یک فروشنده‌ی آنلاین در حال پردازش تراکنش‌های کارت اعتباری است) ممکن است قابل‌قبول نباشد. بنابراین، هنگامی‌که رمزگذاری کلید خصوصی یک گزینه است (یعنی اگر دو طرف بتوانند به‌صورت امن یک کلید را از قبل تسهیم کنند)، آنگاه معمولاً باید از همین گزینه استفاده کرد.

درواقع، همان‌طور که در بخش ۱۱-۳ مشاهده خواهیم کرد، رمزگذاری کلید خصوصی در «موقعیت کلید عمومی» برای بهبود کارایی برای رمزگذاری (کلید عمومی) پیام‌های طولانی، استفاده می‌شود. بنابراین، درک کامل رمزگذاری کلید خصوصی برای درک چگونگی پیاده‌سازی رمزگذاری کلید عمومی در عمل، ضروری است.

توزیع امن کلیدهای عمومی

در تمام بحث خود تا این لحظه، به‌صورت ضمنی فرض کرده‌ایم که متخاصم، «غیرفعال» است؛ یعنی، متخاصم تنها دست به شنود ارتباط بین فرستنده و گیرنده می‌زند ولی «به‌صورت فعال» در ارتباط مداخله نمی‌کند. اگر متخاصم دارای توانایی دست‌کاری «تمام» ارتباط بین طرفین صادق باشد و این طرفین صادق هیچ کلید رمزی را از قبل تسهیم نکرده باشند، آنگاه محرمانگی را اصلاً نمی‌توان به دست آورد. برای مثال، اگر یک گیرنده، آلیس، کلید عمومی خود، pk، را برای باب ارسال کند ولی متخاصم آن را با یک کلید pk' متعلق به خود (که برای آن، کلید خصوصی منطبق sk' را می‌داند) جایگزین کند، آنگاه هرچند باب پیام خود را با استفاده از pk' رمزگذاری می‌کند، متخاصم به‌سادگی قادر به بازیابی پیام (با استفاده از sk') خواهد بود. یک حمله‌ی مشابه، مشمر ثمر خواهد بود اگر متخاصم قادر به تغییر مقدار کلید عمومی آلیس باشد که در یک فهرست عمومی مفروض، ذخیره شده است یا اینکه متخاصم بتواند کلید عمومی را هنگام ارسال از فهرست عمومی به باب، دست‌کاری کند. اگر آلیس و باب هیچ اطلاعاتی را از قبل تسهیم نکنند و مایل به تکیه به یک طرف ثالث مورد اعتماد هر دو، نباشند، آلیس و باب هیچ کاری نمی‌توانند برای جلوگیری از چنین حملاتی و یا حتی تشخیص اینکه چنین حمله‌ای رخ داده است، انجام دهند[۴۲].

نکته‌ی مهم این است که بررسی رمزگذاری کلید عمومی در این فصل، فرض می‌کند که فرستندگان قادر به اکتساب یک کپی قانونی از کلید عمومی گیرنده هستند. (این امر به‌صورت ضمنی در تعاریف

[۴۲] در سناریوی «فریاد زدن از دو سوی اتاق»، آلیس و باب می‌توانند متخاصم مداخله کننده در ارتباط را تشخیص دهند. ولی این امر تنها به این دلایل است که (۱) متخاصم نمی‌تواند مانع رسیدن پیام‌های آلیس به باب شود و (۲) آلیس و باب از قبل اطلاعاتی را «تسهیم» کرده‌اند (برای مثال، صدای صحبت کردن خود) که به آن‌ها اجازه می‌دهد تا ارتباط خود را «احراز اصالت» کنند.

امنیت ارائه‌شده توسط ما، فرض شده است.) یعنی، «توزیع کلید امن» را فرض می‌کنیم. این فرض به این دلیل انجام نشده که حملات فعال بحث شده در بالا، هیچ اهمیتی ندارند-درواقع، این حملات نشان‌دهنده‌ی یک تهدید جدی هستند که در هر سیستم جهان واقعی که از رمزگذاری کلید عمومی بهره می‌برد، باید مدیریت و حل شوند. درواقع، این فرض به این دلیل در نظر گرفته شده است که مکانیسم‌های دیگری برای جلوگیری از حملات فعال (برای مثال ن.ک. بخش ۱۲-۷) وجود دارند و بنابراین جدا نمودن مطالعه‌ی رمزگذاری کلید عمومی امن از مطالعه‌ی توزیع کلید عمومی امن، راحت‌تر (و مفید) است.

۱۱-۲- تعاریف

با تعریف ساختار رمزگذاری کلید عمومی، آغاز می‌کنیم. این تعریف بسیار شبیه به تعریف ۳-۷ است با این تفاوت که به‌جای کار کردن با تنها یک کلید، اکنون دارای کلیدهای رمزگذاری و رمزگشایی متمایز هستیم.

تعریف ۱۱-۱

یک طرح رمزگذاری کلید عمومی یک سه‌گانه از الگوریتم‌های زمان-چندجمله‌ای تصادفی (Gen, Enc, Dec) است به صورتی که:

۱) الگوریتم تولید کلید Gen یک پارامتر امنیتی 1^n را به‌عنوان ورودی دریافت کرده و یک زوج کلید (pk, sk) را به‌عنوان خروجی ارائه می‌کند. ما اولین مورد از این کلیدها را «کلید عمومی» و دومی را «کلید خصوصی» می‌نامیم. برای راحتی کار فرض می‌کنیم که pk و sk هرکدام دارای طول حداقل n هستند و اینکه n را می‌توان از روی pk, sk تعیین نمود.

۲) الگوریتم رمزگذاری Enc به‌عنوان ورودی یک کلید عمومی pk و یک پیام m از یک فضای پیام مفروض (که ممکن است به pk بستگی داشته باشد) را اخذ می‌کند. این الگوریتم، یک متن رمز c را خروجی می‌دهد و ما این امر را به‌صورت $c \leftarrow Enc_{pk}(m)$ می نویسیم. (در ادامه می‌بینیم که Enc باید احتمالاتی باشد تا به امنیت معنادار برسیم.)

۳) الگوریتم رمزگشایی قطعی Dec، به‌عنوان ورودی یک کلید خصوصی sk و یک متن رمز c را دریافت کرده و یک پیام m یا یک علامت خاص $\perp$ نشان‌دهنده‌ی شکست را به‌عنوان خروجی ارائه می‌کند. این عملیات را به‌صورت $m := Dec_{sk}(c)$ می نویسیم.

ضروری است که مگر با احتمال ناچیز بر روی (pk, sk) خروجی توسط $Gen(1^n)$، برای هر پیام (قانونی) m، داشته باشیم $Dec_{sk}\left(Enc_{pk}(m)\right) = m$.

تفاوت مهم با موقعیت کلید خصوصی آن است که اکنون الگوریتم تولید کلید Gen دو کلید را به‌جای یک کلید، خروجی می‌دهد. کلید عمومی pk برای رمزگذاری استفاده می‌شود درحالی‌که کلید

خصوصی sk برای رمزگشایی استفاده می‌شود. در تکرار بحث قبلی خود، فرض بر آن است که pk به‌صورت گسترده توزیع‌شده است به‌گونه‌ای که هرکسی می‌تواند پیام‌ها را برای طرفی که این کلید را تولید کرده است، رمزگذاری کند ولی sk باید توسط گیرنده به‌صورت محرمانه باقی بماند تا امنیت بتواند برقرار بماند.

ما اجازه‌ی یک احتمال ناچیز برای خطای رمزگشایی را می‌دهیم و درواقع بعضی از طرح‌هایی که ارائه می‌کنیم دارای یک احتمال خطای ناچیز هستند (برای مثال اگر نیاز باشد که یک عدد اول انتخاب شود ولی با احتمال ناچیز یک عدد مرکب به دست آید). علی‌رغم این امر، ما معمولاً این مسئله را از اینجا به بعد، نادیده می‌گیریم.

برای استفاده‌ی عملی از رمزگذاری کلید عمومی، می‌خواهیم فضای پیام به‌صورت $\{0,1\}^n$ یا $\{0,1\}^*$ باشد (و علی‌الخصوص، مستقل از کلید عمومی باشد). هرچند گاهی طرح‌های رمزگذاری را با استفاده از فضای پیام $\mathcal{M}$ توصیف می‌کنیم که شامل تمام رشته‌های بیتی با یک طول ثابت مفروض نیست (و اینکه ممکن است همچنین به کلید عمومی بستگی داشته باشد)، در چنین حالت‌هایی چگونگی کدگذاری رشته‌های بیتی به‌صورت عناصر $\mathcal{M}$ را هم مشخص می‌کنیم. این کدگذاری باید هم محاسبه پذیر کارا و هم وارون‌پذیر کارا باشد تا گیرنده بتواند رشته‌ی بیتی رمز شده را بازیابی کند.

۱۱-۲-۱- امنیت علیه حملات مبتنی بر متن اصلی انتخابی

بررسی امنیت را با معرفی همتای «طبیعی» تعریف ۳-۸ در موقعیت کلید عمومی، آغاز می‌کنیم. ازآنجاکه دلایل گسترده‌ای برای این تعریف (و همین‌طور دیگر تعاریفی که مشاهده خواهیم کرد) قبلاً در فصل سوم ارائه‌شده است، بحث اینجا نسبتاً مختصر بوده و ما اصولاً بر تفاوت‌های بین موقعیت‌های کلید خصوصی و کلید عمومی، تمرکز می‌کنیم.

با داشتن یک طرح رمزگذاری کلید عمومی $\Pi = (Gen, Enc, Dec)$ و یک متخاصم $\mathcal{A}$، آزمایش زیر را در نظر بگیرید:

آزمایش تمایزناپذیری شنود $PubK^{eav}_{\mathcal{A},\Pi}(n)$:

۱) متخاصم $\mathcal{A}$ pk را دریافت می‌کند و یک زوج پیام m_0, m_1 با طول برابر در فضای پیام را به‌عنوان خروجی ارائه می‌کند.

۲) یک بیت یکنواخت $b \in \{0,1\}$ انتخاب می‌شود و سپس یک متن رمز $c \leftarrow Enc_{pk}(m_b)$ محاسبه‌شده و به $\mathcal{A}$ داده می‌شود. ما c را متن رمز چالش می‌نامیم.

۳) متخاصم $\mathcal{A}$ یک بیت b' را به‌عنوان خروجی ارائه می‌کند. خروجی آزمایش برابر با ۱ است اگر $b' = b$ و در غیر این صورت برابر با ۰ خواهد بود. اگر $b' = b$ باشد، می‌گوییم $\mathcal{A}$ موفق شده است.

تعریف ۱۱-۲

یک طرح رمزگذاری کلید عمومی $\Pi = (Gen, Enc, Dec)$ دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر است اگر برای تمام متخاصمین زمان-چندجمله‌ای تصادفی $\mathcal{A}$، یک تابع ناچیز $negl$ وجود داشته باشد به صورتی که

$$\Pr[PubK^{eav}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + negl(n).$$

تفاوت اصلی بین تعریف بالا و تعریف ۳-۸ آن است که در اینجا، $\mathcal{A}$ کلید عمومی pk را دریافت می‌کند. به‌علاوه، به $\mathcal{A}$ اجازه می‌دهیم تا پیام‌های m_0 و m_1 خود را بر اساس این کلید عمومی انتخاب کند. هنگام تعریف امنیت رمزگذاری کلید عمومی، این امر ضروری است به این دلیل که همان‌طور که قبلاً بحث شد، فرض می‌کنیم که متخاصم کلید عمومی گیرنده را می‌داند.

تغییر ظاهراً «جزئی» ارائه‌ی کلید عمومی pk که برای رمزگذاری پیام استفاده می‌شود به $\mathcal{A}$ دارای یک اثر عظیم است: این امر اصولاً دسترسی به یک پیشگوی رمزگذاری را به‌رایگان به $\mathcal{A}$ می‌دهد. (مفهوم پیشگوی رمزگذاری در بخش ۳-۴-۲ توضیح داده شده است.) این امر صادق است به این دلیل که متخاصم با داشتن pk می‌تواند هر پیام m را به‌تنهایی و با محاسبه‌ی $Enc_{pk}(m)$ رمزگذاری کند. (مثل همیشه، فرض می‌شود که $\mathcal{A}$ الگوریتم Enc را می‌داند.) نکته‌ی مقابل آن است که تعریف ۱۱-۲ برابر با امنیت-CPA (یعنی امنیت در مقابل حملات مبتنی بر متن اصلی انتخابی) تعریف‌شده به شکلی مشابه با تعریف ۳-۲۲ تنها با این تفاوت است که مهاجم، کلید عمومی را در آزمایش متناظر، دریافت می‌کند. بنابراین، داریم:

گزاره‌ی ۱۱-۳

اگر یک طرح رمزگذاری کلید عمومی دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر باشد، آنگاه CPA-امن است.

این امر متضاد با موقعیت کلید خصوصی است که در آن، طرح‌هایی وجود دارند که دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر هستند ولی تحت یک حمله‌ی مبتنی بر متن اصلی انتخابی، ناامن هستند (ن.ک. گزاره‌ی ۳-۲۰). تفاوت‌های دیگر با موقعیت کلید خصوصی که تقریباً به شکل فوری از مطلب بالا نتیجه می‌شوند، در ادامه موردبحث قرارگرفته‌اند.

غیرممکن بودن رمزگذاری کلید عمومی کاملاً محرمانه

رمزگذاری کلید عمومی کاملاً محرمانه را نمی‌توان به شکل مشابه با تعریف ۲-۳ با مشروط نمودن کل دیدگاه شنودگر (یعنی شامل کلید عمومی) تعریف نمود. به شکل معادل، این مقوله را می‌توان با

تعمیم تعریف ۱۱-۲ تعریف نمود به این صورت که برای تمام متخاصمین $\mathcal{A}$ (و نه‌فقط متخاصمین کارا) ملزم کنیم که داشته باشیم:

$$\Pr[PubK^{eav}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2}.$$

بااین‌حال، برخلاف موقعیت کلید خصوصی، رمزگذاری کلید عمومی کاملاً محرمانه، «غیرممکن» است بدون توجه به اینکه کلیدها چقدر طولانی هستند یا فضای پیام چقدر کوچک است. درواقع، یک متخاصم نامحدود با داشتن pk و یک متن رمز c محاسبه‌شده از طریق $c \leftarrow Enc_{pk}(m)$ می‌تواند m را با احتمال ۱ تعیین کند. اثبات این امر به‌عنوان تمرین ۱۱-۱ در نظر گرفته شده است.

عدم امنیت رمزگذاری کلید عمومی قطعی

همان‌طور که در رابطه با رمزگذاری کلید خصوصی بیان شد، هیچ طرح رمزگذاری قطعی نمی‌تواند CPA-امن باشد. همین اصل در اینجا نیز برقرار است:

قضیه‌ی ۱۱-۴

هیچ طرح رمزگذاری کلید عمومی قطعی، CPA-امن نیست.

به این دلیل که قضیه‌ی ۱۱-۴ بسیار مهم است، باید اندکی بیشتر در مورد آن صحبت کنیم. این قضیه «نتیجه‌ی» تعریف امنیت ما یا نشانه‌ی اینکه تعریف ما بیش‌ازحد قوی است، نیست. طرح‌های رمزگذاری کلید عمومی قطعی در مقابل حملات «عملی» در سناریوهای «واقع‌بینانه»، آسیب‌پذیر هستند و نباید هیچ‌گاه استفاده شوند. دلیل این امر آن است که یک طرح قطعی نه‌تنها به متخاصم اجازه می‌دهد که تعیین کند چه زمانی یک پیام یکتا دو بار ارسال‌شده است (مشابه با موقعیت کلید خصوصی) بلکه همچنین اگر مجموعه‌ی پیام‌های ممکن مورد رمزگذاری، کوچک باشد، به متخاصم اجازه می‌دهد این پیام را با احتمال ۱ بازیابی کند. برای مثال، استادی را در نظر بگیرید که نمرات دانشجویان را رمزگذاری می‌کند. در اینجا، شنودگر می‌داند که نمره‌ی هر دانشجو باید یکی از نمرات $\{A, B, C, D, F\}$ باشد. اگر استاد از یک طرح رمزگذاری کلید عمومی قطعی استفاده کند، شنودگر می‌تواند به‌سرعت نمره‌ی واقعی هر دانشجو را با رمزگذاری تمام نمرات ممکن و مقایسه‌ی نتیجه با متن رمز داده شده، تعیین کند.

هرچند قضیه‌ی بالا به نظر بیش‌ازحد ساده است، برای مدتی طولانی، بسیاری از سیستم‌های جهان واقعی با استفاده از رمزگذاری کلید عمومی قطعی، طراحی شده بودند. می‌توان گفت هنگامی‌که رمزگذاری کلید عمومی معرفی شد، اهمیت رمزگذاری احتمالاتی هنوز به‌طور کامل درک نشده بود. مطالعه‌ی برجسته‌ی گلدواسر و میکالی، که در آن (چیزی معادل با) تعریف ۱۱-۲ پیشنهادشده و قضیه‌ی ۱۱-۴ بیان‌شده بود، نقطه عطفی در حوزه‌ی رمزنگاری به شمار می‌رود. اهمیت مشخص

کردن شهود فردی در یک تعریف رسمی و در نظر گرفتن موارد به شکلی صحیح در بار اول- حتی اگر در آینده مشخص شود که به نظر ساده بوده است- نباید دست‌کم گرفته شود.

۱۱-۲-۲- رمزگذاری‌های چندگانه

مشابه با فصل سوم، درک اثر استفاده از کلید یکسان (در این حالت، کلید عمومی یکسان) برای رمزگذاری پیام‌های چندگانه، مهم است. در چنین موقعیتی، می‌توانیم امنیت را با ملزم کردن یک متخاصم برای اعلام دو «فهرست» از متون اصلی، به‌صورت بیان‌شده در تعریف ۳-۱۹، فرمول‌بندی کنیم. بااین‌حال، به دلایل بحث شده در بخش ۳-۴-۲، به‌جای این کار از تعریفی استفاده می‌کنیم که در آن، مهاجم دسترسی به یک پیشگوی «چپ یا راست» $LR_{pk,b}$ را به دست می‌آورد که با دریافت یک زوج پیام m_0, m_1 با طول برابر به‌عنوان ورودی، متن رمز $c \leftarrow Enc_{pk}(m_b)$ را محاسبه کرده و c را بازمی‌گرداند. مهاجم اجازه دارد به هر تعداد که می‌خواهد، این پیشگو را مورد پرسمان قرار دهد و بنابراین این تعریف، امنیت را زمانی مدل‌سازی می‌کند که چندین پیام (مجهول) با استفاده از کلید عمومی یکسان، رمزگذاری می‌شوند.

به شکل رسمی، آزمایش زیر که برای یک طرح رمزگذاری کلید عمومی $\Pi = (Gen, Enc, Dec)$ و متخاصم $\mathcal{A}$ تعریف شده است را در نظر بگیرید:

آزمایش پیشگوی- LR، $PubK^{LR-cpa}_{\mathcal{A},\Pi}(n)$:

۱) الگوریتم $Gen(1^n)$ اجرا می‌شود تا کلیدهای (pk, sk) به دست آیند.
۲) یک بیت یکنواخت $b \in \{0,1\}$ انتخاب می‌شود.
۳) متخاصم $\mathcal{A}$ به pk ورودی و دسترسی پیشگو به $LR_{pk,b}(\cdot,\cdot)$ را دریافت می‌کند.
۴) متخاصم $\mathcal{A}$ یک بیت b' را به‌عنوان خروجی ارائه می‌کند.
۵) خروجی آزمایش برابر با ۱ تعریف می‌شود اگر $b' = b$ و در غیر این صورت، برابر با ۰ تعریف می‌شود. اگر $PubK^{LR-cpa}_{\mathcal{A},\Pi}(n) = 1$ باشد، می‌گوییم $\mathcal{A}$ موفق شده است.

تعریف ۱۱-۵

یک طرح رمزگذاری کلید عمومی $\Pi = (Gen, Enc, Dec)$ دارای رمزگذاری‌های چندگانه‌ی نمایزناپذیر خواهد بود اگر برای تمام متخاصمین زمان-چندجمله‌ای تصادفی $\mathcal{A}$، یک تابع ناچیز $negl$ وجود داشته باشد به صورتی که:

$$\Pr[PubK^{LR-cpa}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + negl(n).$$

نشان خواهیم داد که هر طرح CPA-امن «به‌صورت خودکار» دارای رمزگذاری‌های چندگانه‌ی نمایزناپذیر خواهد بود؛ یعنی، در موقعیت کلید عمومی، امنیت برای رمزگذاری یک پیام یکتا به‌صورت ضمنی نشان‌دهنده‌ی امنیت برای رمزگذاری پیام‌های چندگانه خواهد بود. این امر به این معنا است

که می‌توانیم امنیت یک طرح مفروض را بر اساس تعریف ۱۱-۲ اثبات کنیم، که ساده‌تر بوده و کار کردن با آن آسان‌تر است، و نتیجه بگیریم که این طرح، در تعریف ۱۱-۵ صدق می‌کند که ظاهراً یک تعریف قوی‌تر است که به شکلی دقیق‌تر کاربرد جهان واقعی رمزگذاری کلید عمومی را مدل‌سازی می‌کند. اثبات قضیه‌ی زیر در ادامه آورده شده است.

قضیه‌ی ۱۱-۶

اگر طرح رمزگذاری کلید عمومی Π دارای امنیت CPA باشد، آنگاه دارای رمزگذاری‌های چندگانه‌ی تمایزناپذیر هم خواهد بود.

یک نتیجه‌ی مشابه در موقعیت کلید خصوصی به‌عنوان قضیه‌ی ۳-۲۴ بیان شد ولی اثبات نشد.

رمزگذاری پیام‌های با طول دلخواه

یک نتیجه‌ی فوری قضیه‌ی ۱۱-۶ آن است که یک طرح رمزگذاری کلید عمومی CPA-امن برای پیام‌های با طول ثابت به شکل ضمنی نشان‌دهنده‌ی یک طرح رمزگذاری کلید عمومی برای پیام‌های با طول دلخواه است که در همین مفهوم امنیت صدق می‌کند. ما این امر را در حالت نهایی نشان می‌دهیم که در آن، طرح اولیه تنها پیام‌های ۱-بیتی را رمزگذاری می‌کند. فرض کنید $\Pi = (Gen, Enc, Dec)$ یک طرح رمزگذاری برای پیام‌های تک-بیتی باشد. می‌توانیم یک طرح جدید $\Pi' = (Gen, Enc', Dec')$ را ایجاد کنیم که دارای فضای پیام $\{0,1\}^*$ باشد به این صورت که Enc' را به شکل زیر تعریف کنیم:

$$\mathrm{Enc}'_{pk}(m) = \mathrm{Enc}_{pk}(m_1), \ldots, \mathrm{Enc}_{pk}(m_t), \qquad (11.1)$$

که در آن، $m = m_1 \cdots m_t$. (الگوریتم رمزگشایی Dec' به شکل بدیهی ساخته می‌شود.) داریم:

ادعای ۱۱-۷

فرض کنید Π و Π' به شکل تعریف‌شده‌ی بالا باشند. اگر Π دارای امنیت CPA باشد، آنگاه Π' هم CPA-امن خواهد بود.

این ادعا از آنجا نتیجه می‌شود که می‌توانیم رمزگذاری یک پیام m با استفاده از Π' را به‌عنوان یک رمزگذاری از t پیام $(m_1, \ldots, m_t)$ با استفاده از طرح Π در نظر بگیریم.

نکته‌ای در خصوص لغات استفاده‌شده

سه تعریف از امنیت را برای طرح‌های رمزگذاری کلید عمومی ارائه کرده‌ایم- رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر، امنیت CPA و رمزگذاری‌های چندگانه‌ی تمایزناپذیر-که همگی باهم معادل هستند. بر اساس قاعده‌ی معمول در ادبیات رمزنگاری، تنها از عبارت «امنیت CPA» برای اشاره به طرح‌های صادق در این مفاهیم امنیت استفاده خواهیم کرد.

اثبات قضیه‌ی ۱۱-۶

اثبات قضیه‌ی ۱۱-۶ تا حدی پیشرفته است. بنابراین، قبل از پرداختن به جزئیات، اندکی برداشت شهودی ارائه می‌کنیم. برای این بحث شهودی، برای سادگی فرض می‌کنیم که $\mathcal{A}$ تنها دو فراخوان از پیشگوی LR در آزمایش $PubK^{LR-cpa}_{\mathcal{A},\Pi}(n)$ انجام می‌دهد. (در اثبات کامل، تعداد فراخوان‌ها، اختیاری است.)

یک متخاصم PPT دلخواه $\mathcal{A}$ و یک طرح رمزگذاری کلید عمومی CPA-امن Π را مشخص کنید و یک آزمایش $PubK^{LR-cpa_2}_{\mathcal{A},\Pi}(n)$ را در نظر بگیرید که در آن، $\square$ تنها می‌تواند دو پرسمان از پیشگوی LR بپرسد. پرسمان‌های درخواست شده توسط $\mathcal{A}$ از پیشگو را به‌صورت $(m_{1,0}, m_{1,1})$ و $(m_{2,0}, m_{2,1})$ نشان دهید؛ توجه کنید که دومین زوج پیام‌ها ممکن است به اولین متن رمز دریافت شده توسط $\mathcal{A}$ از پیشگو، بستگی داشته باشد. در این آزمایش، $\mathcal{A}$ یا یک زوج متن رمز $(\mathrm{Enc}_{pk}(m_{1,0}), \mathrm{Enc}_{pk}(m_{2,0}))$ (اگر $b = 0$) یا یک زوج متن رمز $(\mathrm{Enc}_{pk}(m_{1,1}), \mathrm{Enc}_{pk}(m_{2,1}))$ (اگر $b = 1$) را دریافت می‌کند. برای نشان دادن خروجی $\mathcal{A}$ در حالت اول می نویسیم $\mathcal{A}(pk, \mathrm{Enc}_{pk}(m_{1,0}), \mathrm{Enc}_{pk}(m_{2,0}))$ و برای حالت دوم هم از عبارت مشابهی استفاده می‌کنیم.

فرض کنید $\vec{C}_0$ نشان‌دهنده‌ی توزیع زوج متن رمزها در حالت اول و $\vec{C}_1$ نشان‌دهنده‌ی توزیع زوج متن رمزها در حالت دوم باشد. برای نشان دادن اینکه تعریف ۱۱-۵ (برای $PubK^{LR-cpa_2}_{\square,\Pi}$) برقرار است، باید اثبات کنیم که $\mathcal{A}$ نمی‌تواند بین دریافت یک زوج متن رمز توزیع‌شده بر اساس $\vec{C}_0$ یا یک زوج متن رمز توزیع‌شده بر اساس $\vec{C}_1$ تمایز قائل شود. یعنی، باید اثبات کنیم که یک تابع ناچیز $negl$ وجود دارد به صورتی که

$$\left|\Pr\left[\mathcal{A}(pk, \mathrm{Enc}_{pk}(m_{1,0}), \mathrm{Enc}_{pk}(m_{2,0})) = 1\right] - \Pr\left[\mathcal{A}(pk, \mathrm{Enc}_{pk}(m_{1,1}), \mathrm{Enc}_{pk}(m_{2,1})) = 1\right]\right| \leq negl(n). \qquad (11.2)$$

(این امر معادل با تعریف ۱۱-۵ به همان دلیلی است که تعریف ۳-۹ با تعریف ۳-۸ معادل است.) برای اثبات این امر، نشان می‌دهیم که

۱) CPA-امن بودن Π به شکل ضمنی نشان می‌دهد که $\mathcal{A}$ نمی‌تواند بین حالتی که یک زوج متن رمز توزیع‌شده بر اساس $\vec{C}_0$ یا یک زوج متن رمز $(\mathrm{Enc}_{pk}(m_{1,0}), \mathrm{Enc}_{pk}(m_{2,0}))$ را دریافت می‌کند، که متناظر با رمزگذاری پیام اول در اولین پرسمان پیشگوی $\mathcal{A}$ و دومین پیام در پرسمان پیشگوی دوم $\mathcal{A}$ است، تمایز قائل شود. (هرچند این امر نمی‌تواند در $PubK^{LR-cpa_2}_{\mathcal{A},\Pi}(n)$ رخ دهد، همچنان می‌توانیم ببرسیم که رفتار $\mathcal{A}$ به چه صورت خواهد بود اگر چنین زوج متن رمزی را دریافت کند.) فرض کنید $\vec{C}_0$ نشان‌دهنده‌ی توزیع زوج متن رمزها در این حالت دوم باشد.

۲) به شکل مشابه، CPA-امن بودن Π به شکل ضمنی نشان می‌دهد که $\mathcal{A}$ نمی‌تواند بین حالتی که یک زوج متن رمز توزیع‌شده بر اساس $\vec{C}_{\cdot}$ دریافت می‌کند با حالتی که یک زوج متن رمز توزیع‌شده بر اساس $\vec{C}_{1}$ دریافت می‌کند، تمایز قائل شود.

مطلب بالا بیان می‌کند که $\mathcal{A}$ نمی‌تواند بین توزیع‌های $\vec{C}_{\cdot}$ و $\vec{C}_{1}$ یا بین توزیع‌های $\vec{C}_{\cdot}$ و $\vec{C}_{1}$ تمایز قائل شود. نتیجه می‌گیریم (با استفاده از جبر ساده) که $\mathcal{A}$ نمی‌تواند بین توزیع‌های $\vec{C}_{\cdot}$ و $\vec{C}_{1}$ تمایز قائل شود.

بنابراین، بخش سخت این اثبات نشان دادن این امر است که $\mathcal{A}$ نمی‌تواند بین دریافت یک زوج متن رمز توزیع‌شده بر اساس $\vec{C}_{\cdot}$ یا یک زوج متن رمز توزیع‌شده بر اساس $\vec{C}_{1}$ تمایز قائل شود. (حالت دیگر به شکل مشابه نتیجه می‌شود.) یعنی، می‌خواهیم نشان دهیم که یک تابع ناچیز $negl$ وجود دارد که برای آن

$$\left|\Pr\left[\mathcal{A}(pk, \mathrm{Enc}_{pk}(m_{1,\cdot}), \mathrm{Enc}_{pk}(m_{2,\cdot})) = 1\right] - \Pr\left[\mathcal{A}(pk, \mathrm{Enc}_{pk}(m_{1,\cdot}), \mathrm{Enc}_{pk}(m_{2,1})) = 1\right]\right| \leq negl(n) \qquad (11.3)$$

توجه کنید که تنها تفاوت بین ورودی متخاصم $\mathcal{A}$ در هر حالت، در عنصر دوم است. به شکل شهودی، تمایزناپذیری از حالت تک پیام نتیجه می‌شود چراکه خود $\mathcal{A}$ می‌تواند $\mathrm{Enc}_{pk}(m_{1,\cdot})$ را تولید کند. به شکل رسمی، متخاصم PPT زیر، $\mathcal{A}'$، را در نظر بگیرید که در آزمایش $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A}',\Pi}(n)$ اجرا می‌شود:

متخاصم $\mathcal{A}'$

۱) با دریافت ورودی pk، متخاصم $\mathcal{A}'$ $\mathcal{A}(pk)$ را به‌عنوان یک زیرروال اجرا می‌کند.

۲) هنگامی‌که $\mathcal{A}$ اولین پرسمان $(m_{1,\cdot}, m_{1,1})$ خود را از پیشگوی LR می‌پرسد، $\mathcal{A}'$ مقدار $c_1 \leftarrow \mathrm{Enc}_{pk}(m_{1,\cdot})$ را محاسبه کرده و c_1 را به‌عنوان پاسخ از سوی پیشگو، به $\mathcal{A}$ بازمی‌گرداند.

۳) $\mathcal{A}'$ بیت b' خروجی توسط $\mathcal{A}$ را به‌عنوان خروجی ارائه می‌کند.

با نگاهی به آزمایش $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A}',\Pi}(n)$، مشاهده می‌کنیم که زمانی که $b = \cdot$ باشد، متن رمز چالش c_2 به‌صورت $\mathrm{Enc}_{pk}(m_{2,\cdot})$ محاسبه می‌شود. بنابراین،

$$\Pr\left[\mathcal{A}'(\mathrm{Enc}_{pk}(m_{2,\cdot})) = 1\right] = \Pr\left[\mathcal{A}(\mathrm{Enc}_{pk}(m_{1,\cdot}), \mathrm{Enc}_{pk}(m_{2,\cdot})) = 1\right]. \qquad (11.4)$$

(اشاره‌ی آشکار به pk را برای صرفه‌جویی در فضا، حذف می‌کنیم.) در مقابل، زمانی که $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A}',\Pi}(n)$، $b = 1$ باشد، آنگاه c_2 به‌صورت $\mathrm{Enc}_{pk}(m_{2,1})$ محاسبه می‌شود و بنابراین

$$\Pr\left[\mathcal{A}'(\mathrm{Enc}_{pk}(m_{2,1})) = 1\right] = \Pr\left[\mathcal{A}(\mathrm{Enc}_{pk}(m_{1,\cdot}), \mathrm{Enc}_{pk}(m_{2,1})) = 1\right]. \qquad (11.5)$$

CPA-امن بودن Π به شکل ضمنی نشان می‌دهد که یک تابع ناچیز $negl$ وجود دارد به صورتی که

$$\left|\Pr\left[\mathcal{A}'(\mathrm{Enc}_{pk}(m_{2,\cdot})) = 1\right] - \Pr\left[\mathcal{A}'(\mathrm{Enc}_{pk}(m_{2,1})) = 1\right]\right| \leq negl(n).$$

این امر به همراه معادلات (۱۱.۴) و (۱۱.۵)، معادله‌ی (۱۱.۳) را می‌دهد.

تقریباً به شکلی یکسان، می‌توانیم اثبات کنیم که:

$$\left|\Pr\left[\mathcal{A}(pk, \mathrm{Enc}_{pk}(m_{1,\cdot}), \mathrm{Enc}_{pk}(m_{2,1})) = 1\right] - \Pr\left[\mathcal{A}(pk, \mathrm{Enc}_{pk}(m_{1,1}), \mathrm{Enc}_{pk}(m_{2,1})) = 1\right]\right| \leq negl(n). \qquad (11.6)$$

معادله‌ی (۱۱.۲) با ترکیب کردن معادلات (۱۱.۳) و (۱۱.۶) به دست می‌آید.

اصلی‌ترین مشکلی که در حالت اولیه به وجود می‌آید آن است که تعداد پرسمان‌ها از پیشگوی LR دیگر ثابت نیست بلکه ممکن است یک چندجمله‌ای دلخواه از n باشد. در اثبات رسمی، این مسئله با استفاده از یک استدلال ترکیبی حل می‌شود. (استدلالات ترکیبی در فصل هفتم هم مورد استفاده قرار گرفتند.)

اثبات (قضیه‌ی ۱۱-۶)

فرض کنید Π یک طرح رمزگذاری کلید عمومی CPA-امن و $\mathcal{A}$ یک متخاصم PPT دلخواه در آزمایش $PubK^{LR-cpa}_{\mathcal{A},\Pi}(n)$ باشد. فرض کنید $t = t(n)$ یک کران بالای چندجمله‌ای بر روی تعداد پرسمان‌های انجام شده توسط $\mathcal{A}$ از پیشگوی LR باشد و بدون کاستن از کلیت فرض کنید که $\mathcal{A}$ همواره پیشگو را دقیقاً این تعداد دفعات مورد پرسمان قرار می‌دهد. برای یک کلید عمومی مفروض pk و $0 \leq i \leq t$، فرض کنید LR^i_{pk} نشان‌دهنده‌ی پیشگویی باشد که با دریافت ورودی $(m_{\cdot}, m_{1})$ برای اولین i پرسمان دریافتی، $\mathrm{Enc}_{pk}(m_{\cdot})$ را بازمی‌گرداند و برای $t - i$ پرسمان بعدی که دریافت می‌کند، $\mathrm{Enc}_{pk}(m_{1})$ را بازمی‌گرداند. (یعنی، برای اولین i پرسمان، اولین پیام در زوج ورودی رمزگذاری می‌شود و در پاسخ به مابقی پرسمان‌ها، دومین پیام در زوج ورودی، رمزگذاری می‌شود.) تأکید می‌کنیم که هر رمزگذاری با استفاده از مقدار تصادفی یکنواخت مستقل، محاسبه می‌شود. با استفاده از این نمادگذاری، داریم

$$\Pr\left[PubK^{LR-cpa}_{\mathcal{A},\Pi}(n) = 1\right] = \frac{1}{2}\cdot\Pr\left[\mathcal{A}^{\mathrm{LR}^t_{pk}}(pk) = \cdot\right] + \frac{1}{2}\cdot\Pr\left[\mathcal{A}^{\mathrm{LR}^{\cdot}_{pk}}(pk) = 1\right]$$

به این دلیل که از دیدگاه $\mathcal{A}$ (که دقیقاً t پرسمان انجام می‌دهد)، پیشگوی LR^t_{pk} معادل با $LR_{pk,\cdot}$ و پیشگوی $\mathrm{LR}^{\cdot}_{pk}$ معادل با $LR_{pk,1}$ است. به‌منظور اثبات اینکه Π در تعریف ۱۱-۵ صدق می‌کند، نشان می‌دهیم که برای هر PPT $\mathcal{A}$، یک تابع ناچیز $negl'$ وجود دارد به صورتی که

$$\left|\Pr\left[\mathcal{A}^{\mathrm{LR}^t_{pk}}(pk) = 1\right] - \Pr\left[\mathcal{A}^{\mathrm{LR}^{\cdot}_{pk}}(pk) = 1\right]\right| \leq negl'(n). \qquad (11.7)$$

(به‌مانند قبل، این نتیجه معادل با تعریف ۱۱-۵ است به همان دلیلی که تعریف ۳-۹ معادل با تعریف ۳-۸ است.)

متخاصم PPT زیر، $\mathcal{A}'$، را در نظر بگیرید که رمزگذاری یک پیام یکتا را شنود می‌کند:

متخاصم $\mathcal{A}'$

۱) متخاصم $\mathcal{A}'$ با دریافت pk، یک نمایه‌ی یکنواخت $i \leftarrow \{1, \dots, t\}$ را انتخاب می‌کند.

۲) متخاصم $\mathcal{A}'$، $\mathcal{A}(pk)$ را اجرا می‌کند و پرسمان پیشگوی jام خود، یعنی $(m_{j,0}, m_{j,1})$ را به‌صورت زیر پاسخ می‌دهد:

(الف) برای $j = i$، متخاصم $\mathcal{A}'$، $c_j \leftarrow \mathrm{Enc}_{pk}(m_{j,0})$ را محاسبه کرده و c_j را به‌عنوان پاسخ از سوی پیشگوی خود برای $\mathcal{A}$ بازمی‌گرداند.

(ب) برای $j = i$، متخاصم $\mathcal{A}'$ خروجی $(m_{j,0}, m_{j,1})$ را ارائه کرده و یک متن رمز چالش c_j را در پاسخ دریافت می‌کند. این مقوله به‌عنوان پاسخ از سوی پیشگوی خود برای $\mathcal{A}$ بازگردانده می‌شود.

(ج) برای $j > i$، متخاصم $\mathcal{A}'$ مقدار $c_j \leftarrow \mathrm{Enc}_{pk}(m_{j,1})$ را محاسبه کرده و c_j را به‌عنوان پاسخ از سوی پیشگوی خود برای $\mathcal{A}$ بازمی‌گرداند.

۳) متخاصم $\mathcal{A}'$ بیت b' خروجی توسط $\mathcal{A}$ را به‌عنوان خروجی ارائه می‌کند.

آزمایش $PubK^{eav}_{\mathcal{A}',\Pi}(n)$ را در نظر بگیرید. با مشخص کردن یک انتخاب مفروض از $i = i^*$، توجه کنید که اگر $c_{i^*,0}$ یک رمزگذاری از $m_{i^*,0}$ باشد، آنگاه تعامل $\mathcal{A}$ با پیشگوی خود با تعامل با پیشگوی $\mathrm{LR}^{i^*}_{pk}$ معادل خواهد بود. بنابراین،

$$\begin{aligned}\Pr[\mathcal{A}' \text{ outputs } 1 | b = 0] &= \sum_{i^*=1}^{t} \Pr[i = i^*] \cdot \Pr[\mathcal{A}' \text{ outputs } 1 | b = 0 \wedge i = i^*] \\ &= \sum_{i^*=1}^{t} \frac{1}{t} \cdot \Pr\left[\mathcal{A}^{\mathrm{LR}^{i^*}_{pk}}(pk) = 1\right].\end{aligned}$$

از سوی دیگر، اگر $c_{i^*,0}$ یک رمزگذاری از $m_{i^*,1}$ باشد، آنگاه تعامل $\mathcal{A}$ با پیشگوی خود با تعامل با پیشگوی $LR^{i^*-1}_{pk}$ معادل خواهد بود و بنابراین

$$\begin{aligned}\Pr[\mathcal{A}' \text{ outputs } 1 | b = 1] &= \sum_{i^*=1}^{t} \Pr[i = i^*] \cdot \Pr[\mathcal{A}' \text{ outputs } 1 | b = 1 \wedge i = i^*] \\ &= \sum_{i^*=1}^{t} \frac{1}{t} \cdot \Pr\left[\mathcal{A}^{LR^{i^*-1}_{pk}}(pk) = 1\right] \\ &= \sum_{i^*=0}^{t-1} \frac{1}{t} \cdot \Pr\left[\mathcal{A}^{\mathrm{LR}^{i^*}_{pk}}(pk) = 1\right],\end{aligned}$$

که در آن، تساوی سوم تنها با انتقال نمایه‌های جمع، به دست می‌آید.

ازآنجاکه $\mathcal{A}'$ در زمان چندجمله‌ای اجرا می‌شود، این فرض که Π، CPA-امن است به این معنا است که یک تابع ناچیز $negl$ وجود دارد به صورتی که

$$|\Pr[\mathcal{A}' \text{ outputs } 1 | b = 0] - \Pr[A' \text{ outputs } 1 | b = 1]| \leq negl(n).$$

ولی این امر به این معناست که

$$\begin{aligned}negl(n) &\geq \left| \sum_{i^*=1}^{t} \frac{1}{t} \cdot \Pr\left[\mathcal{A}^{\mathrm{LR}^{i^*}_{pk}}(pk) = 1\right] - \sum_{i^*=0}^{t-1} \frac{1}{t} \cdot \Pr\left[\mathcal{A}^{\mathrm{LR}^{i^*}_{pk}}(pk) = 1\right] \right| \\ &= \frac{1}{t} \cdot \left| \Pr\left[\mathcal{A}^{\mathrm{LR}^{t}_{pk}}(pk) = 1\right] - \Pr\left[\mathcal{A}^{\mathrm{LR}^{0}_{pk}}(pk) = 1\right] \right|,\end{aligned}$$

ازآنجاکه همه‌ی جملات به‌غیراز یکی در هر جمع باهم خنثی می‌شوند، نتیجه می‌گیریم که

$$\left| \Pr\left[\mathcal{A}^{\mathrm{LR}^{t}_{pk}}(pk) = 1\right] - \Pr\left[\mathcal{A}^{\mathrm{LR}^{0}_{pk}}(pk) = 1\right] \right| \leq t(n).negl(n).$$

به این دلیل که t چندجمله‌ای است، تابع $t.negl(n)$ ناچیز است. ازآنجاکه $\mathcal{A}$ یک متخاصم PPT دلخواه بود، این امر نشان می‌دهد که معادله‌ی (۱۱.۷) برقرار است و بنابراین اثبات اینکه Π دارای رمزگذاری‌های چندگانه‌ی تمایزناپذیر است، کامل می‌شود. ■

۱۱-۲-۳- امنیت علیه حملات متن رمز منتخب

حملات متن رمز منتخب، که در آن‌ها، متخاصم قادر به کسب رمزگشایی متون رمز دلخواه انتخابی خود است (با یک محدودیت فنی که در ادامه توصیف شده است)، در موقعیت کلید عمومی به‌مانند موقعیت کلید خصوصی، یک دغدغه به شمار می‌روند. درواقع، می‌توان استدلال کرد که این حملات در موقعیت کلید عمومی، باعث دغدغه‌ی بیشتری هم هستند چراکه در این موقعیت، گیرنده انتظار دارد متون رمز را از چندین فرستنده دریافت کند که احتمالاً از قبل معلوم نیستند درحالی‌که یک گیرنده در موقعیت کلید خصوصی می‌خواهد تنها با یک فرستنده‌ی یکتای معلوم با استفاده از یک کلید رمز خاص، ارتباط برقرار کند.

یک شنودگری $\mathcal{A}$ را فرض کنید که یک متن رمز c ارسال‌شده توسط یک فرستنده‌ی $\mathcal{S}$ به یک گیرنده‌ی $\mathcal{R}$ را مشاهده می‌کند. به‌طورکلی، در موقعیت کلید عمومی، دو دسته از حملات متن رمز منتخب وجود دارد:

- $\mathcal{A}$ ممکن است یک متن رمز تغییریافته‌ی c' را از سوی $\mathcal{S}$ برای $\mathcal{R}$ ارسال کند. (برای مثال، در رابطه با ایمیل رمز شده ، $\mathcal{A}$ ممکن است یک ایمیل رمز شده ی c' را ساخته و فیلد «*From*» را به صورتی جعل نماید که به نظر برسد ایمیل از سوی $\mathcal{S}$ فرستاده شده است.) در این حالت، هرچند این احتمال کم است که $\mathcal{A}$ قادر به اکتساب کل رمزگشایی m' برای c' شود، ممکن است برای $\mathcal{A}$ این امکان وجود داشته باشد که مقداری اطلاعات در خصوص

m' بر اساس رفتار بعدی $\mathcal{R}$ به دست آورد. بر اساس این اطلاعات، $\mathcal{A}$ ممکن است قادر به یادگرفتن چیزی در مورد پیام اصلی m باشد.

- $\mathcal{A}$ ممکن است یک متن رمز تغییریافته‌ی c' را به نام خود برای $\mathcal{R}$ ارسال کند. در این حالت، $\mathcal{A}$ ممکن است کل رمزگشایی m' برای c' را به دست آورد اگر $\mathcal{R}$ به‌صورت مستقیم به $\mathcal{A}$ پاسخ دهد. حتی اگر $\mathcal{A}$ هیچ‌چیزی در مورد m' نفهمد، این پیام تغییریافته ممکن است دارای یک رابطه‌ی معلوم با پیام اولیه‌ی m باشد که بتواند توسط $\mathcal{A}$ مورد سوءاستفاده قرار گیرد؛ برای مثال ن.ک. سناریوی ذیل.

دسته‌ی دوم حملات مخصوص حالت رمزگذاری کلید عمومی است و هیچ مشابهی در وضعیت کلید خصوصی ندارد.

شناسایی تعدادی سناریوی واقع‌بینانه که نشان‌دهنده‌ی انواع حملات بالا باشند، دشوار نیست:

سناریوی اول

فرض کنید کاربر $\mathcal{S}$ با ارسال یک رمزگذاری از گذرواژه pw خود که یک مهر زمانی به آن الصاق شده است به بانک خود، وارد حساب بانکی خود شود. همچنین فرض کنید که دو نوع پیام خطا وجود دارند که بانک ارسال می‌کند: اگر گذرواژه‌ی رمز شده منطبق با گذرواژه‌ی ذخیره شده برای $\mathcal{S}$ نباشد، بانک پیام «*password incorrect*» (گذرواژه اشتباه است) را بازمی‌گرداند و اگر گذرواژه درست باشد ولی مهر زمانی درست نباشد، بانک، پیام خطای «*timestamp incorrect*» (مهر زمانی اشتباه است) را بازمی‌گرداند.

اگر متخاصم یک متن رمز c ارسال‌شده توسط $\mathcal{S}$ به بانک را به دست آورد، می‌تواند یک حمله‌ی متن رمز منتخب را با ارسال متن رمزهای c' به بانک از سوی $\mathcal{S}$ و مشاهده‌ی پیام‌های خطای ارائه‌شده، ساماندهی نماید. (این روش مشابه با حمله‌ی مبتنی بر پیشگوی لایی گذاری شده است که در بخش ۳-۷-۲ مشاهده کردیم.) در بعضی موارد، این اطلاعات ممکن است کافی باشد که متخاصم کل گذرواژه‌ی کاربر را تعیین کند.

سناریوی دوم

فرض کنید $\mathcal{S}$ یک ایمیل رمز شده c را برای $\mathcal{R}$ ارسال می‌کند و این ایمیل توسط $\mathcal{A}$ مشاهده می‌شود. اگر $\mathcal{A}$ یک ایمیل رمز شده ی c' را با نام خود به $\mathcal{R}$ ارسال کند، آنگاه $\mathcal{R}$ ممکن است به این ایمیل پاسخ داده و متن رمزگشایی‌شده‌ی m' متناظر با c' را نقل‌قول نماید. در این حالت، $\mathcal{R}$ اصولاً به‌عنوان یک پیشگوی رمزگشایی برای $\mathcal{A}$ عمل می‌کند و ممکن است به‌صورت بالقوه هر متن رمزی را که $\mathcal{A}$ برای آن ارسال می‌کند، رمزگشایی کند.

سناریوی سوم

مسئله‌ای که ارتباط نزدیکی با مسئله‌ی امنیت متن رمز منتخب دارد عبارت است از شکل‌پذیری یا قابلیت‌های متون رمز. ازآنجاکه تعریف رسمی بسیار پیچیده است، در اینجا چنین تعریفی ارائه نمی‌کنیم بلکه فقط یک ایده‌ی شهودی را ارائه می‌نماییم. یک طرح، «شکل‌پذیر» است اگر دارای ویژگی زیر باشد: با داشتن یک رمزگذاری c از یک پیام نامعلوم m مفروض، می‌توان یک متن رمز c' را به دست آورد که یک رمزگذاری از یک پیام m' باشد که به «شکل معلوم مرتبط با m است». برای مثال، شاید با داشتن یک رمزگذاری از m، این امر امکان داشته باشد که یک رمزگذاری از $2m$ را ایجاد کنیم. (مثال‌های طبیعی از طرح‌های CPA-امن دارای این ویژگی و ویژگی‌های مشابه را بعداً مشاهده می‌کنیم؛ ن.ک. بخش ۱۳-۲-۳.)

اکنون تصور کنید که $\mathcal{R}$ در حال اجرای یک مزایده است که در آن دو طرف $\mathcal{S}$ و $\mathcal{A}$ پیشنهادهای خود را با رمزگذاری آن‌ها با استفاده از کلید عمومی $\mathcal{R}$ ارسال می‌کنند. اگر یک طرح رمزگذاری شکل‌پذیر استفاده شود، ممکن است برای متخاصم $\mathcal{A}$ این امکان به وجود آید که همواره بالاترین پیشنهاد را ارائه کند (بدون اینکه مقدار حداکثر را پیشنهاد نماید) به این صورت که حمله‌ی زیر را اجرا نماید: صبر کنید تا $\mathcal{S}$ یک متن رمز c' متناظر با پیشنهاد خود، یعنی m (که برای $\mathcal{A}$ نامعلوم است) را ارسال نماید؛ سپس، یک متن رمز c' متناظر با پیشنهاد $m' = 2m$ را ارسال کنید. توجه کنید که m (و درواقع، m') برای $\mathcal{A}$ نامعلوم باقی می‌مانند تا زمانی که $\mathcal{R}$ نتایج را اعلام می‌کند و بنابراین احتمال چنین حمله‌ای نقض‌کننده‌ی این واقعیت نیست که طرح رمزگذاری، CPA-امن است. ازسوی دیگر، می‌توان نشان داد که طرح‌های CPA-امن، شکل ناپذیر هستند به این معنا که در برابر چنین حملاتی، آسیب‌پذیر نیستند.

تعریف

امنیت در مقابل حملات متن رمز منتخب از طریق تغییر مناسب در تعریف مشابه بیان‌شده در وضعیت کلید خصوصی (تعریف ۳-۳۳) تعریف می‌شود. با داشتن یک طرح رمزگذاری کلید عمومی Π و یک متخاصم $\mathcal{A}$ آزمایش زیر را در نظر بگیرید:

آزمایش تمایزناپذیری CCA، $PubK^{cca}_{\mathcal{A},\Pi}(n)$:

۱) الگوریتم $Gen(1^n)$ اجرا می‌شود تا کلیدهای (pk, sk) به دست آیند.

۲) متخاصم $\mathcal{A}$، مقدار pk و دسترسی به یک پیشگوی رمزگشایی $Dec_{sk}(\cdot)$ را دریافت می‌کند. این متخاصم یک زوج پیام m_0, m_1 با طول یکسان را به‌عنوان خروجی ارائه می‌کند. (این پیام‌ها باید در فضای پیام مرتبط با pk قرار داشته باشند.)

۳) یک بیت یکنواخت $b \in \{0, 1\}$ انتخاب می‌شود و سپس یک متن رمز $c \leftarrow Enc_{pk}(m_b)$ محاسبه‌شده و به $\mathcal{A}$ داده می‌شود.

۴) $\mathcal{A}$ به تعامل خود با پیشگوی رمزگشایی ادامه می‌دهد ولی نمی‌تواند رمزگشایی خود c را درخواست کند. درنهایت، $\mathcal{A}$، یک بیت b' را به‌عنوان خروجی ارائه می‌دهد.

۵) خروجی آزمایش برابر با ۱ تعریف می‌شود اگر $b = b'$ و در غیر این صورت، برابر با ۰ تعریف خواهد شد.

تعریف ۱۱-۸

یک طرح رمزگذاری کلید عمومی $\Pi = (Gen, Enc, Dec)$ دارای رمزگذاری‌های تمایزناپذیر تحت یک حمله‌ی متن رمز منتخب است (یا CCA-امن است) اگر برای تمام متخاصمین زمان-چندجمله‌ای تصادفی $\mathcal{A}$، یک تابع ناچیز $negl$ وجود داشته باشد به‌گونه‌ای که

$$\Pr[PubK^{cca}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + negl(n).$$

مشابه طبیعی قضیه‌ی ۱۱-۶ برای امنیت CCA هم برقرار است. یعنی، اگر یک طرح دارای رمزگذاری‌های تمایزناپذیر تحت یک حمله‌ی متن رمز منتخب باشد، آنگاه دارای رمزگذاری‌های چندگانه‌ی تمایزناپذیر تحت یک حمله‌ی متن رمز منتخب خواهد بود که در آن، این مقوله به شکل مناسب تعریف شده است. بااین‌حال، جالب اینجاست که مشابه ادعای ۱۱-۷ برای امنیت CCA برقرار نخواهد بود.

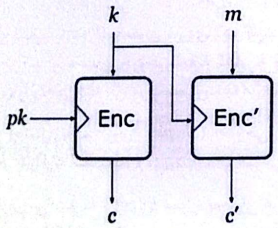
مشابه با تعریف ۳-۳۳، ما باید مانع مهاجم برای ارسال متن رمز چالش c به پیشگوی رمزگشایی شویم تا این تعریف قابل‌دستیابی باشد. ولی این محدودیت باعث بی‌معنا شدن تعریف نخواهد شد و علی‌الخصوص، برای هرکدام از سه سناریوی تأثیرگذار که قبلاً ارائه شدند، می‌توان استدلال نمود که قرار دادن $c' = c$ هیچ سودی برای مهاجم نخواهد داشت:

- در سناریوی اول مربوط به ورود با استفاده از گذرواژه، مهاجم هیچ‌چیزی در مورد گذرواژه‌ی s با بازگرداندن c به بانک نمی‌فهمد چراکه در این حالت، از قبل می‌داند که هیچ پیام خطایی تولید نخواهد شد.
- در سناریوی دوم مربوط به ایمیل رمز شده ، ارسال $c' = c$ به گیرنده به‌احتمال‌زیاد باعث می‌شود که گیرنده مشکوک شود و بنابراین اصلاً پاسخی ارائه نکند.
- در سناریوی سوم مربوط به مزایده، $\mathcal{R}$ به‌سادگی می‌تواند تقلب را تشخیص دهد اگر پیشنهاد رمز شده ی متخاصم مشابه با پیشنهاد رمز شده ی طرف دیگر باشد. به‌هرحال، در این حالت، تنها چیزی که مهاجم با ارسال c به دست می‌آورد آن است که پیشنهادی یکسان با پیشنهاد طرف صادق را ارسال خواهد نمود.

۱۱-۳- رمزگذاری ترکیبی و الگوی KEM/DEM

ادعای ۱۱-۷ نشان می‌دهد که هر طرح رمزگذاری کلید عمومی CPA-امن برای پیام‌های l'-بیتی را می‌توان برای به دست آوردن یک طرح رمزگذاری کلید عمومی CPA-امن برای پیام‌های با طول دلخواه، استفاده نمود. رمزگذاری یک پیام l-بیتی با استفاده از این رویکرد، نیازمند $\gamma \stackrel{def}{=} \lceil l/l' \rceil$ فراخوان از طرح رمزگذاری اولیه است، به این معنا که هم محاسبه و هم طول متن رمز توسط یک عامل ضرب γ متناسب به طرح مبنا، افزایش می یابند.

با استفاده از رمزگذاری کلید خصوصی «همراه با» رمزگذاری کلید عمومی، می‌توانیم عملکرد بهتری داشته باشیم. این امر باعث بهبود کارایی می‌شود چراکه رمزگذاری کلید خصوصی به شکل چشم‌گیری سریع‌تر از رمزگذاری کلید عمومی است و پهنای باند را بهبود می‌بخشد به این دلیل که طرح‌های کلید خصوصی دارای توسیع متن رمز پایین‌تری هستند. ترکیب به‌دست‌آمده را «رمزگذاری ترکیبی» می‌نامند و به‌صورت گسترده در عمل، مورداستفاده قرار می‌گیرد. ایده‌ی اساسی عبارت است از استفاده از رمزگذاری کلید عمومی برای به دست آوردن یک کلید تسهیمی k و سپس رمزگذاری پیام m با استفاده از یک طرح رمزگذاری کلید خصوصی و کلید k. گیرنده از کلید خصوصی (نامتقارن) بلندمدت خود برای به دست آوردن k استفاده می‌کند و سپس از رمزگشایی کلید خصوصی (با کلید k) برای بازیابی پیام اولیه، استفاده می‌کند. تأکید می‌کنیم که هرچند رمزگذاری کلید خصوصی به‌عنوان یک مکمل استفاده می‌شود، این مقوله یک طرح رمزگذاری کلید عمومی کامل است بر این اساس که فرستنده و گیرنده «از قبل» هیچ کلید رمزی را تسهیم نمی‌کنند.



تصویر ۱۱-۱: رمزگذاری ترکیبی. Enc نشان‌دهنده‌ی یک طرح رمزگذاری کلید عمومی است درحالی‌که Enc' یک طرح رمزگذاری کلید خصوصی است.

در یک پیاده‌سازی مستقیم از این ایده (ن.ک. تصویر ۱۱-۱)، فرستنده کلید k را با (۱) انتخاب یک مقدار یکنواخت k و سپس (۲) رمزگذاری k با استفاده از یک طرح رمزگذاری کلید عمومی، تسهیم می‌کند. یک رویکرد مستقیم‌تر عبارت است از استفاده از یک پایه‌ی کلید عمومی به نام «مکانیسم

لفافه بندی کلید» (*KEM*) برای انجام هر دو این موارد «در یک حرکت». این شیوه هم از دیدگاه مفهومی و هم از دیدگاه کارایی، مفید است، همان‌طور که در ادامه خواهیم دید.

یک *KEM* دارای سه الگوریتم است که ماهیتی مشابه با الگوریتم‌های طرح رمزگذاری کلید عمومی دارند. به‌مانند قبل، الگوریتم تولید کلید *Gen* برای تولید یک زوج کلید عمومی و خصوصی، استفاده می‌شود. به‌جای رمزگذاری، اکنون یک الگوریتم «لفافه بندی» *Encaps* داریم که تنها یک کلید عمومی (بدون پیام) را به‌عنوان ورودی دریافت می‌کند و یک متن رمز c همراه با یک کلید k را به‌عنوان خروجی ارائه می‌کند. یک الگوریتم «لفافه زدایی» متناظر، *Decaps*، توسط گیرنده اجرا می‌شود تا k از روی متن رمز c با استفاده از کلید خصوصی، بازیابی شود. به شکل رسمی:

تعریف ۱۱-۹

یک مکانیسم لفافه بندی کلید (*KEM*) یک چندگانه از الگوریتم‌های زمان-چندجمله ای احتمالاتی $(Gen, Encaps, Decaps)$ است به گونه ای که:

۱) الگوریتم تولید کلید *Gen* به‌عنوان ورودی، پارامتر امنیتی 1^n را دریافت کرده و یک زوج کلید عمومی/خصوصی (pk, sk) را به‌عنوان خروجی ارائه می‌کند. فرض می‌کنیم که pk و sk هرکدام دارای طول حداقل n هستند و اینکه n را می‌توان از روی pk تعیین نمود.

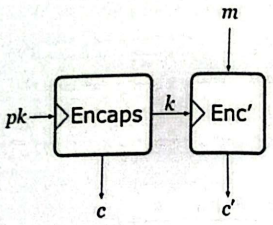
۲) الگوریتم لفافه بندی *Encaps* به‌عنوان ورودی، یک کلید عمومی pk و پارامتر امنیتی 1^n را دریافت می‌کند. این الگوریتم به‌عنوان خروجی، یک متن رمز c و یک کلید $k \in \{0,1\}^{l(n)}$ را ارائه می‌کند که در آن، l طول کلید است. این امر را به‌صورت $(c,k) \leftarrow Encaps_{pk}(1^n)$ می نویسیم.

۳) الگوریتم لفافه زدایی قطعی *Decaps* به‌عنوان ورودی یک کلید خصوصی sk و یک متن رمز c را دریافت می‌کند و به‌عنوان خروجی، یک کلید k یا یک علامت خاص $\perp$ نشان‌دهنده‌ی شکست را ارائه می‌کند. این امر را به‌صورت $k := Decaps_{sk}(c)$ می نویسیم.

ضروری است که مگر با احتمال ناچیز روی (sk, pk) خروجی توسط $Gen(1^n)$، اگر $Encaps_{pk}(1^n)$ خروجی (c,k) را ارائه کند، آنگاه $Decaps_{sk}(c)$ خروجی k را ارائه کند.

در این تعریف، برای سادگی فرض می‌کنیم که *Encaps* همواره به‌عنوان خروجی (یک متن رمز c و) یک کلید با طول ثابت مفروض $l(n)$ را ارائه می‌کند. همچنین می‌توان یک تعریف عمومی‌تر را در نظر گرفت که در آن، *Encaps* مقدار 1^l را به‌عنوان یک ورودی اضافی دریافت کرده و یک کلید با طول l را به‌عنوان خروجی ارائه می‌کند.

هر طرح رمزگذاری کلید عمومی به‌صورت بدیهی یک *KEM* را با انتخاب یک کلید تصادفی k و رمزگذاری آن، می‌دهد. بااین‌حال، همان‌طور که خواهیم دید، ساختارهای اختصاصی برای *KEM*ها می‌توانند کارایی بیشتری داشته باشند.



تصویر ۱۱-۲: رمزگذاری ترکیبی با استفاده از رویکرد *KEM/DEM*

با استفاده از یک *KEM* (با طول کلید n) می‌توانیم رمزگذاری ترکیبی را به‌صورت نشان داده‌شده در تصویر ۱۱-۲، پیاده‌سازی کنیم. فرستنده، $Encaps_{pk}(1^n)$ را برای به دست آوردن c به همراه یک کلید k اجرا می‌کند؛ در ادامه از یک طرح رمزگذاری کلید خصوصی برای رمزگذاری پیام m خود، با استفاده از k به‌عنوان کلید، استفاده می‌کند. در این وضعیت، طرح رمزگذاری کلید خصوصی را به دلایل واضح، «مکانیسم لفافه بندی داده» (*DEM*) می‌نامند. متن رمز فرستاده شده به گیرنده شامل c و همین‌طور متن رمز c' از طرح کلید خصوصی، است. ساختار ۱۱-۱۰ مشخصات رسمی را می‌دهد.

رمزگذاری ترکیبی با استفاده از الگوی *KEM/DEM*

ساختار ۱۱-۱۰

فرض کنید $\Pi = (Gen, Encaps, Decaps)$ یک *KEM* با طول کلید n و $\Pi' = (Gen', Enc', Dec')$ یک طرح رمزگذاری کلید خصوصی باشد. یک طرح رمزگذاری کلید عمومی $\Pi^{hy} = (Gen^{hy}, Enc^{hy}, Dec^{hy})$ را به‌صورت زیر، ایجاد کنید:

- Gen^{hy}: با دریافت 1^n به‌عنوان ورودی، $Gen(1^n)$ را اجرا کرده و کلیدهای عمومی و خصوصی (pk, sk) اعلام شده، استفاده کنید.
- Enc^{hy}: با دریافت یک کلید عمومی pk و یک پیام $m \in \{0,1\}^*$ به‌عنوان ورودی، موارد زیر را انجام دهید:
  (۱) محاسبه‌ی $(c,k) \leftarrow \text{Encaps}_{pk}(1^n)$.
  (۲) محاسبه‌ی $c' \leftarrow \text{Enc}'_k(m)$.
  (۳) ارائه‌ی متن رمز $\langle c, c' \rangle$ به‌عنوان خروجی.
- Dec^{hy}: با دریافت یک کلید خصوصی sk و یک متن رمز $\langle c, c' \rangle$ به‌عنوان ورودی، موارد زیر را انجام دهید:
  (۱) محاسبه‌ی $k := \text{Decaps}_{sk}(c)$.
  (۲) ارائه‌ی پیام $m := \text{Dec}'_k(c')$ به‌عنوان خروجی.

کارایی طرح رمزگذاری ترکیبی Π^{hy} به‌دست‌آمده، چیست؟ برای یک مقدار ثابت مفروض n، فرض کنید α نشان‌دهنده‌ی هزینه‌ی لفافه بندی کلید n-بیتی با استفاده از $Encaps$ باشد و فرض کنید β نشان‌دهنده‌ی هزینه‌ی (برای هر بیت متن اصلی) رمزگذاری با استفاده از Enc' باشد. فرض کنید که $|m| > n$، که حالت جالب‌توجه است. آنگاه، برای هر بیت متن اصلی، هزینه‌ی رمزگذاری یک پیام m با استفاده از Π^{hy} برابر است با

$$\frac{\alpha + \beta \cdot |m|}{|m|} = \frac{\alpha}{|m|} + \beta, \qquad (11.8)$$

که برای m به‌اندازه‌ی کافی طولانی، به β میل می‌کند. آنگاه، در حد پیام‌های بسیار طولانی، هزینه‌ی هر بیت ایجادشده توسط طرح رمزگذاری کلید عمومی Π^{hy} برابر با هزینه برای هر بیت در طرح کلید خصوصی Π' است. بنابراین، رمزگذاری ترکیبی به ما اجازه می‌دهد که به «عملکرد» رمزگذاری کلید عمومی در کارایی رمزگذاری کلید خصوصی، حداقل برای پیام‌های به‌اندازه‌ی کافی طولانی، برسیم.

یک محاسبه‌ی مشابه را می‌توان برای اندازه‌گیری اثر رمزگذاری ترکیبی بر روی طول متن رمز مورداستفاده قرار داد. برای یک مقدار ثابت مفروض n، فرض کنید L نشان‌دهنده‌ی طول متن رمز خروجی توسط $Encaps$ باشد و فرض کنید رمزگذاری کلید خصوصی یک پیام m با استفاده از Enc' منجر به یک متن رمز با طول $|m| + n$ شود (این امر را می‌توان با استفاده از یکی از سبک‌های رمزگذاری موردبحث در بخش ۳-۶ به دست آورد؛ درواقع، حتی طول متن رمز $|m|$ هم ممکن است چراکه همان‌طور که مشاهده خواهیم کرد نیازی نیست که Π' دارای امنیت CPA باشد). آنگاه، طول کل یک متن رمز در طرح Π^{hy} برابر است با

$$L + n + |m|. \qquad (11.9)$$

در مقابل، هنگام استفاده از رمزگذاری قالب به قالب به شکل معادله‌ی (۱۱.۱) و با این فرض که رمزگذاری کلید عمومی یک پیام n-بیتی با استفاده از Enc منجر به یک متن رمز با طول L خواهد شد، رمزگذاری یک پیام m منجر به یک متن رمز با طول $L \cdot \lceil |m|/n \rceil$ خواهد شد. طول متن رمز گزارش‌شده در معادله‌ی (۱۱.۹) بهبودی چشم‌گیری برای m به‌اندازه‌ی کافی طولانی است.

می‌توانیم از تخمین‌های تقریبی برای درک بهتر معنای نتایج بالا در عمل استفاده کنیم. (تأکید می‌کنیم که هدف از بیان این ارقام تنها ارائه‌ی یک درک کلی برای این بهبود به خواننده است؛ مقادیر واقع‌بینانه به مجموعه‌ی گسترده‌ای از عوامل بستگی خواهند داشت.) یک مقدار معمول برای طول کلید k می‌تواند $n = 128$ باشد. به‌علاوه، یک طرح رمزگذاری کلید عمومی «اختصاصی» ممکن است هنگام رمزگذاری پیام‌های ۱۲۸-بیتی، متون رمز ۲۵۶-بیتی را به دست دهد؛ فرض کنید یک KEM دارای متون رمز با طول برابر هنگام لفافه بندی یک کلید ۱۲۸-بیتی است. با این فرض که به‌مانند

قبل α نشان‌دهنده‌ی هزینه‌ی محاسباتی رمزگذاری/لفافه بندی کلید عمومی یک کلید ۱۲۸-بیتی است، مشاهده می‌کنیم که رمزگذاری قالب-به-قالب به شکل معادله‌ی (۱۱.۱)، یک پیام یک مگابایتی (2^{20}-بیتی) را با هزینه‌ی محاسباتی $\alpha \cdot \lceil 2^{20}/128 \rceil \approx 7800 \cdot \alpha$ رمزگذاری کرده و متن رمز دارای طول MB ۲ خواهد بود. این امر را با کارایی رمزگذاری ترکیبی مقایسه کنید. با این فرض که به‌مانند قبل، β نشان‌دهنده‌ی هزینه‌ی محاسباتی در بیت برای رمزگذاری کلید خصوصی است، یک تخمین منطقی عبارت است از $\beta \approx \alpha/10^5$. با استفاده از معادله‌ی (۱۱.۸)، مشاهده می‌کنیم که هزینه‌ی محاسباتی کلی برای رمزگذاری ترکیبی برای یک پیام Mb ۱ برابر است با

$$\alpha + 10^6 \cdot \frac{\alpha}{10^5} = 11 \cdot \alpha,$$

و متن رمز تنها اندکی طولانی‌تر از MB ۱ خواهد بود. بنابراین، رمزگذاری ترکیبی باعث بهبود کارایی محاسباتی در این حالت به‌اندازه‌ی یک ضریب ۷۰۰ و طول متن رمز به‌اندازه‌ی یک ضریب ۲، می‌شود.

اکنون باید امنیت Π^{hy} را هم تحلیل کنیم. این امر البته به امنیت مؤلفه‌های مبنای آن، یعنی Π و Π' بستگی خواهد داشت. در بخش‌های زیر، ما مفاهیم CPA-امن بودن و CCA-امن بودن را برای KEMها تعریف کرده و نشان می‌دهیم:

- اگر Π یک KEM دارای امنیت CPA باشد و طرح کلید خصوصی Π' دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر باشد، آنگاه Π^{hy} یک طرح رمزگذاری کلید عمومی CPA-امن خواهد بود. توجه کنید که کافی است Π' یک در تعریف ضعیف‌تر برای امنیت صدق کند-که یادآوری می‌کنیم به معنای امنیت CPA در موقعیت کلید خصوصی نیست- تا طرح ترکیبی Π^{hy} دارای امنیت CPA باشد. به شکل شهودی، دلیل این امر آن است که یک کلید یکنواخت «تازه» k هر بار که یک پیام جدید رمزگذاری می‌شود، انتخاب می‌گردد. ازآنجاکه هر کلید k تنها یک‌بار استفاده می‌شود، تمایزناپذیری یک رمزگذاری یکتا از Π' برای امنیت طرح ترکیبی Π^{hy} کافی است. این امر به این معنا است که رمزگذاری کلید خصوصی اساسی با استفاده از یک مولد شبه تصادفی (یا رمز دنباله‌ای)، مثل ساختار ۳-۱۷، کافی است.
- اگر Π یک KEM دارای امنیت CCA باشد و Π' یک طرح رمزگذاری کلید خصوصی CCA-امن باشد، آنگاه Π^{hy} یک طرح رمزگذاری کلید عمومی CCA-امن خواهد بود.

۱۱-۲-۱- امنیت CPA

برای سادگی، در این بخش و بخش بعدی، یک KEM با طول کلید n را فرض می‌کنیم. مفهومی از امنیت CPA را برای KEMها بر اساس مشابهت با تعریف ۱۱-۲ تعریف می‌کنیم. به‌مانند آن تعریف، نخاصم در اینجا یک متن رمز یکتای c را شنود می‌کند. تعریف ۱۱-۲ ملزم می‌کند که مهاجم قادر

به تمایز اینکه آیا c یک رمزگذاری از یک پیام مفروض $m.$ یا یک پیام دیگر m_1 است، نخواهد بود. در یک KEM، هیچ پیامی وجود ندارد و به‌جای این الزام، بیان می‌کنیم که کلید لفافه بندی شده k از یک کلید یکنواخت که مستقل از متن رمز c است، تمایزناپذیر نیست.

فرض کنید $\Pi = (Gen, Encaps, Decaps)$ یک KEM بوده و $\mathcal{A}$ یک متخاصم دلخواه باشد.

آزمایش تمایزناپذیری CPA: $KEM^{cpa}_{\mathcal{A},\Pi}(n)$

۱) $Gen(1^n)$ اجرا می‌شود تا کلیدهای (pk, sk) به دست آیند. آنگاه، $Encaps_{pk}(1^n)$ اجرا می‌شود تا (c, k) با $k \in \{0,1\}^n$ تولید شود.

۲) یک بیت یکنواخت $b \in \{0,1\}$ انتخاب می‌شود. اگر $b = 0$ باشد، قرار می‌دهیم $\hat{k} := k$. اگر $b = 1$ باشد، آنگاه یک $\hat{k} \in \{0,1\}^n$ یکنواخت را انتخاب می‌کنیم.

۳) $(pk, c, \hat{k})$ را به $\mathcal{A}$ می‌دهیم که یک بیت b' را به‌عنوان خروجی ارائه می‌کند. خروجی آزمایش برابر با ۱ تعریف می‌شود اگر $b' = b$ و در غیر این صورت، برابر با ۰ تعریف خواهد شد.

در این آزمایش، $\mathcal{A}$ متن رمز c و یا کلید واقعی k متناظر با c یا یک کلید مستقل یکنواخت را دریافت می‌کند. KEM به‌صورت CPA-امن خواهد بود اگر هیچ متخاصم کارایی نتواند بین این حالات ممکن، تمایز قائل شود.

تعریف ۱۱-۱۱

یک مکانیسم لفافه بندی کلید Π به‌صورت CPA-امن است اگر برای تمام متخاصمین زمان-چندجمله ای احتمالاتی $\mathcal{A}$، یک تابع ناچیز $negl$ وجود داشته باشد به صورتی که:

$$\Pr[KEM^{cpa}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + negl(n).$$

در مابقی این بخش، قضیه‌ی ذیل را اثبات می‌کنیم:

قضیه‌ی ۱۱-۱۲

اگر Π یک KEM دارای امنیت CPA و Π' یک طرح رمزگذاری کلید خصوصی باشد که دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر است، آنگاه Π^{hy} تعریف‌شده در ساختار ۱۱-۱۰، یک طرح رمزگذاری کلید عمومی CPA-امن خواهد بود.

قبل از اثبات *رسمی این* قضیه، اندکی اطلاعات شهودی ارائه می‌کنیم. فرض کنید نماد «$X \overset{c}{\equiv} Y$» نشان‌دهنده‌ی این رخداد باشد که هیچ متخاصم زمان-چندجمله ای نتواند بین دو توزیع X و Y تمایز قائل شود. (این مفهوم به شکلی رسمی‌تر در بخش ۷-۸ بررسی می‌شود هرچند ما در اینجا به مطالب آن پخش تکیه نمی‌کنیم.) برای مثال، فرض کنید $\text{Encaps}^{(1)}_{pk}(1^n)$ (به ترتیب، $(\text{Encaps}^{(2)}_{pk}(1^n)$) نشان‌دهنده‌ی متن رمز (به ترتیب، کلید) خروجی توسط $Encaps$ باشد. این واقعیت که Π به‌صورت CPA-امن است به این معنا است که

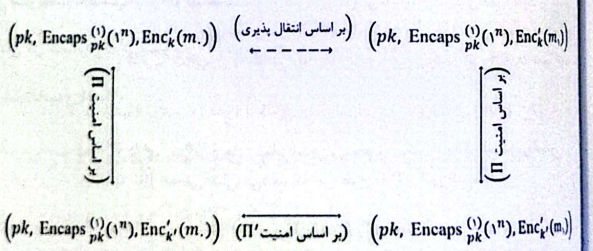
$$\left(pk, \text{Encaps}^{(1)}_{pk}(1^n), \text{Encaps}^{(2)}_{pk}(1^n)\right) \overset{c}{\equiv} \left(pk, \text{Encaps}^{(1)}_{pk}(1^n), k'\right),$$

که در آن، pk توسط $Gen(1^n)$ تولید می‌شود و k' به‌صورت مستقل و یکنواخت از $\{0,1\}^n$ انتخاب می‌شود. به شکل مشابه، این واقعیت که Π' دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر است به این معنا است که برای هر m_0, m_1 خروجی توسط $\mathcal{A}$ اگر k به‌صورت یکنواخت و تصادفی انتخاب شده باشد، خواهیم داشت $\text{Enc}'_k(m_0) \overset{c}{\equiv} \text{Enc}'_k(m_1)$.

به‌منظور اثبات CPA-امن بودن Π^{hy} باید نشان دهیم که برای m_0, m_1 خروجی توسط یک متخاصم PPT $\mathcal{A}$:

$$\left(pk, \text{Encaps}^{(1)}_{pk}(1^n), \text{Enc}'_k(m_0)\right) \overset{c}{\equiv} \left(pk, \text{Encaps}^{(1)}_{pk}(1^n), \text{Enc}'_k(m_1)\right) \quad (11.10)$$

(معادله‌ی (۱۱.۱۰) برای نشان دادن اینکه Π^{hy} دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر است، کافی است و بر اساس گزاره‌ی ۱۱-۳، این امر به شکل ضمنی نشان می‌دهد که Π^{hy} دارای امنیت CPA است.)



تصویر ۱۱-۳: ساختار سطح بالای اثبات قضیه‌ی ۱۱-۱۲ (پیکان‌ها نشان‌دهنده‌ی تمایزناپذیری هستند)

اثبات در سه گام ادامه می‌یابد. (ن.ک. تصویر ۱۱-۳.) ابتدا اثبات می‌کنیم که

$$\left(pk,\ \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_k(m.)\right) \overset{c}{\equiv} \left(pk,\ \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_{k'}(m.)\right), \quad (11.11)$$

که در آن، در سمت چپ، k توسط $Encaps_{pk}^{(2)}(1^n)$ اعلام می‌شود و در سمت راست، k' یک کلید یکنواخت مستقل است. این امر از طریق یک کاهش نسبتاً سرراست نتیجه می‌شود چراکه CPA-امن بودن Π دقیقاً به این معنا است که $Encaps_{pk}^{(2)}(1^n)$ را نمی‌توان از یک کلید k' یکنواخت متمایز نمود حتی با داشتن pk و $Encaps_{pk}^{(1)}(1^n)$.

در ادامه، اثبات می‌کنیم که

$$\left(pk,\ \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_k(m.)\right) \overset{c}{\equiv} \left(pk,\ \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_{k'}(m_1)\right), \quad (11.12)$$

در اینجا تفاوت بین رمزگذاری $m.$ یا m_1 با استفاده از Π' و یک کلید یکنواخت مستقل k' است. بنابراین، معادله‌ی (۱۱.۱۲) از این واقعیت نتیجه می‌شود که Π' دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر است.

دقیقاً به‌مانند حالت معادله‌ی (۱۱.۱۱)، همچنین می‌توانیم نشان دهیم که

$$\left(pk,\ \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_k(m_1)\right) \overset{c}{\equiv} \left(pk,\ \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_{k'}(m_1)\right), \quad (11.13)$$

بازهم با تکیه بر CPA-امن بودن Π. معادلات (۱۱.۱۱) تا (۱۱.۱۳) بر اساس انتقال‌پذیری به‌صورت ضمنی نتیجه‌ی مطلوب معادله‌ی (۱۱.۱۰) را نشان می‌دهند. (انتقال‌پذیری در اثباتی که در ادامه ارائه می‌کنیم به‌صورت ضمنی فرض خواهد شد.)

اکنون کل اثبات را ارائه می‌کنیم.

اثبات (قضیه‌ی ۱۱-۱۲)

اثبات می‌کنیم که Π^{hy} دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر است؛ بر اساس گزاره‌ی ۱۱-۳، این امر به شکل ضمنی نشان می‌دهد که این طرح، CPA-امن است.

یک متخاصم PPT دلخواه $\mathcal{A}^{hy}$ و آزمایش $PubK^{eav}_{\mathcal{A}^{hy},\Pi^{hy}}(n)$ را در نظر بگیرید. هدف ما اثبات این امر است که یک تابع ناچیز negl وجود دارد به صورتی که

$$\Pr\left[PubK^{eav}_{\mathcal{A}^{hy},\Pi^{hy}}(n) = 1\right] \leq \frac{1}{2} + \text{negl}(n).$$

بر اساس تعریف آزمایش، داریم

$$\begin{aligned}&\Pr\left[PubK^{eav}_{\mathcal{A}^{hy},\Pi^{hy}}(n) = 1\right] \quad (11.14)\\ &= \frac{1}{2}.\Pr\left[\mathcal{A}^{hy}\left(pk, \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_k(m.)\right) = 0\right]\\ &+ \frac{1}{2}.\Pr\left[\mathcal{A}^{hy}(pk, \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_k(m_1)) = 1\right],\end{aligned}$$

که در آن، در هر حالت، k برابر با $Encaps_{pk}^{(2)}(1^n)$ است. متخاصم PPT زیر، $\mathcal{A}_1$ که به Π حمله می‌کند را در نظر بگیرید.

۱) $\mathcal{A}_1$ مقادیر $(pk, c, \hat{k})$ را دریافت می‌کند.

۲) $\mathcal{A}_1$ $\mathcal{A}^{hy}(pk)$ را اجرا می‌کند تا دو پیام m_0, m_1 را به دست آورد. سپس، $\mathcal{A}_1$ مقدار $c' \leftarrow \text{Enc}'_{\hat{k}}(m.)$ را محاسبه کرده، متن رمز $\langle c, c'\rangle$ را به $\mathcal{A}^{hy}$ می‌دهد و بیت b' خروجی از $\mathcal{A}^{hy}$ را به‌عنوان خروجی ارائه می‌کند.

رفتار $\mathcal{A}_1$ هنگام حمله به Π در آزمایش $\text{KEM}^{cpa}_{\mathcal{A}_1,\Pi}(n)$ را در نظر بگیرید. هنگامی‌که در این آزمایش، $b = 0$ است، $\mathcal{A}_1$ به $(pk, c, \hat{k})$ داده می‌شود که در آن، هم c و هم $\hat{k}$ توسط $Encaps_{pk}(1^n)$ به‌عنوان خروجی ارائه می‌شوند. این امر به این معنا است که $\mathcal{A}^{hy}$ یک متن رمز به شکل $\langle c, c'\rangle = \langle c, \text{Enc}'_{\hat{k}}(m.)\rangle$ را دریافت می‌کند که در آن، k عبارت است از کلید لفافه بندی شده توسط c. بنابراین،

$$\Pr[\mathcal{A}_1\ outputs\ 0 | b = 0] = \Pr\left[\mathcal{A}^{hy}(pk, \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_k(m.)) = 0\right].$$

از سوی دیگر، زمانی که در آزمایش $\text{KEM}^{cpa}_{\mathcal{A}_1,\Pi}(n)$ داشته باشیم $b = 1$، آنگاه $(pk, c, \hat{k})$ با یکنواخت و مستقل از c به $\mathcal{A}_1$ داده می‌شود. اگر چنین کلیدی را با k' نشان دهیم، این امر به این معناست که $\mathcal{A}^{hy}$ یک متن رمز به شکل $\langle c, \text{Enc}'_{k'}(m.)\rangle$ را دریافت می‌کند و

$$\Pr[\mathcal{A}_1\ outputs\ 1 | b = 1] = \Pr\left[\mathcal{A}^{hy}(pk, \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_{k'}(m.)) = 1\right].$$

ازآنجاکه Π یک KEM دارای امنیت CPA است، یک تابع ناچیز $negl_1$ وجود دارد به صورتی که

$$\begin{aligned}\frac{1}{2} + negl_1(n) &\geq \Pr\left[\text{KEM}^{cpa}_{\mathcal{A}_1,\Pi}(n) = 1\right] \quad (11.15)\\ &= \frac{1}{2}.\Pr[\mathcal{A}_1\ outputs\ 0 | b = 0] + \frac{1}{2}.\Pr[\mathcal{A}_1\ outputs\ 1 | b = 1]\\ &= \frac{1}{2}.\Pr\left[\mathcal{A}^{hy}(pk, \text{Encaps}_{pk}^{(1)}(1^n), \text{Enc}'_k(m.)) = 0\right]\end{aligned}$$

$$+\frac{1}{2}.\Pr\left[A^{hy}(pk, \text{Encaps}^{(1)}_{pk}(1^n), \text{Enc}'_{k'}(m.)) = 1\right]$$

که در آن، k برابر با $Encaps^{(2)}_{pk}(1^n)$ بوده و k' یک کلید یکنواخت و مستقل است.

در ادامه، متخاصم PPT زیر، $\mathcal{A}'$ را در نظر بگیرید که یک پیام رمز شده با استفاده از طرح کلید خصوصی Π' را شنود می‌کند.

متخاصم $\mathcal{A}'$

۱) $\mathcal{A}'(1^n)$ الگوریتم $Gen(1^n)$ را به‌تنهایی اجرا می‌کند تا کلیدهای (pk, sk) را تولید کند. همچنین $c \leftarrow \text{Encaps}^{(1)}_{pk}(1^n)$ را محاسبه می‌کند.

۲) $\mathcal{A}'$ $\mathcal{A}^{hy}(pk)$ را اجرا می‌کند تا دو پیام $m., m_1$ را به دست آورد. این پیام‌ها توسط $\mathcal{A}'$ به‌عنوان خروجی ارائه می‌شوند و در مقابل یک متن رمز c' به آن داده می‌شود.

۳) $\mathcal{A}'$ متن رمز $\langle c, c'\rangle$ را به $\mathcal{A}^{hy}$ می‌دهد و بیت b' را که $\mathcal{A}^{hy}$ خروجی می‌دهد، به‌عنوان خروجی ارائه می‌دهد.

هنگامی‌که در آزمایش $PrivK^{eav}_{\mathcal{A}',\Pi'}(n)$ داشته باشیم $b = 0$، آنگاه متخاصم $\mathcal{A}'$ یک متن رمز c' را دریافت می‌کند که یک رمزگذاری از $m.$ با استفاده از یک کلید k' است که یکنواخت و مستقل از هر چیز دیگری است. بنابراین، یک متن رمز به شکل $\langle c, \text{Enc}'_{k'}(m.)\rangle$ به $\mathcal{A}^{hy}$ داده می‌شود که در آن، k' یکنواخت و مستقل از c است و

$$\Pr[\mathcal{A}' outputs\ 0 | b = 0] = \Pr\left[\mathcal{A}^{hy}(pk, \text{Encaps}^{(1)}_{pk}(1^n), \text{Enc}'_{k'}(m.)) = 0\right].$$

از سوی دیگر، هنگامی‌که در آزمایش $PrivK^{eav}_{\mathcal{A}',\Pi'}(n)$ داشته باشیم $b = 1$، آنگاه $\mathcal{A}'$ یک رمزگذاری از m_1 با استفاده از یک کلید k' یکنواخت و مستقل، دریافت می‌کند. این بدان معناست که $\mathcal{A}^{hy}$ یک متن رمز به شکل $\langle c, \text{Enc}'_{k'}(m_1)\rangle$ را دریافت می‌کند و بنابراین

$$\Pr[\mathcal{A}' outputs\ 1 | b = 1] = \Pr\left[\mathcal{A}^{hy}(pk, \text{Encaps}^{(1)}_{pk}(1^n), \text{Enc}'_{k'}(m_1)) = 1\right].$$

ازآنجاکه Π' دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر است، یک تابع ناچیز $negl'$ وجود دارد به صورتی که

$$\begin{aligned}\frac{1}{2} + negl'(n) &\geq \Pr[PrivK^{eav}_{\mathcal{A}',\Pi'}(n) = 1] \qquad (11.16)\\ &= \frac{1}{2}.\Pr[\mathcal{A}' outputs\ 0 | b = 0] + \frac{1}{2}.\Pr[\mathcal{A}' outputs\ 1 | b = 0]\\ &= \frac{1}{2}.\Pr\left[\mathcal{A}^{hy}(pk, \text{Encaps}^{(1)}_{pk}(1^n), \text{Enc}'_{k'}(m.)) = 0\right]\end{aligned}$$

$$+\frac{1}{2}.\Pr\left[\mathcal{A}^{hy}(pk, \text{Encaps}^{(1)}_{pk}(1^n), \text{Enc}'_{k'}(m_1)) = 1\right].$$

با ادامه‌ی محاسبات دقیقاً به همان صورتی که برای اثبات معادله‌ی (۱۱.۱۵) انجام دادیم، می‌توانیم نشان دهیم که یک تابع ناچیز $negl_2$ وجود دارد به صورتی که

$$\begin{aligned}\frac{1}{2} + negl_2(n) &\geq \Pr\left[\text{KEM}^{cpa}_{\mathcal{A}_2,\Pi}(n) = 1\right] \qquad (11.17)\\ &= \frac{1}{2}.\Pr[\mathcal{A}_2\ outputs\ 0 | b = 0] + \frac{1}{2}.\Pr[\mathcal{A}_2\ outputs\ 1 | b = 0]\\ &= \frac{1}{2}.\Pr\left[\mathcal{A}^{hy}(pk, \text{Encaps}^{(1)}_{pk}(1^n), \text{Enc}'_{k}(m_1)) = 1\right]\\ &+\frac{1}{2}.\Pr\left[\mathcal{A}^{hy}(pk, \text{Encaps}^{(1)}_{pk}(1^n), \text{Enc}'_{k'}(m_1)) = 0\right].\end{aligned}$$

با جمع زدن معادلات (۱۱.۱۵) تا (۱۱.۱۷) و استفاده از این واقعیت که جمع سه تابع ناچیز، ناچیز است، مشاهده می‌کنیم که یک تابع ناچیز $negl$ وجود دارد به صورتی که

$$\begin{aligned}&\frac{3}{2} + negl(n) \geq\\ &\frac{1}{2}.(\Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_k(m.)) = 0] + \Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_{k'}(m.)) = 1]\\ &+\Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_{k'}(m.)) = 0] + \Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_{k'}(m_1)) = 1]\\ &+\Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_k(m_1)) = 1] + \Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_{k'}(m_1)) = 0]),\end{aligned}$$

که در آن، $c = \text{Encaps}^{(1)}_{pk}(1^n)$ در تمام موارد بالا. توجه کنید که

$$\Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_{k'}(m.)) = 1] + \Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_{k'}(m.)) = 0] = 1,$$

ازآنجاکه مجموع احتمالات رخدادهای مکمل همواره برابر با یک است. به شکل مشابه،

$$\Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_{k'}(m_1)) = 1] + \Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_{k'}(m_1)) = 0] = 1.$$

بنابراین،

$$\begin{aligned}&\frac{1}{2} + negl(n)\\ &\geq \frac{1}{2}.(\Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_k(m.)) = 0] + \Pr[\mathcal{A}^{hy}(pk, c, \text{Enc}'_k(m_1)) = 1])\\ &= \Pr\left[PubK^{eav}_{\mathcal{A}^{hy},\Pi^{hy}}(n) = 1\right]\end{aligned}$$

(با استفاده از معادله‌ی (۱۱.۱۴) برای تساوی آخر)، که قضیه را اثبات می‌کند. ■

۱۱-۳-۲- امنیت CCA

اگر خود طرح رمزگذاری کلید خصوصی Π' در برابر حملات متن رمز منتخب، امن نباشد، آنگاه (بدون توجه به KEM استفاده‌شده) طرح رمزگذاری ترکیبی Π^{hy} به‌دست‌آمده هم امن نخواهد بود. به‌عنوان یک مثال ساده‌ی آگاهی‌بخش، فرض کنید که ساختار ۳-۱۷ را به‌عنوان طرح رمزگذاری کلید خصوصی خود در نظر می‌گیریم. آنگاه، بدون مشخص کردن KEM، رمزگذاری یک پیام m توسط Π^{hy} با محاسبه‌ی $(c,k) \leftarrow Encaps_{pk}(1^n)$ و سپس اعلام متن رمز زیر انجام می‌شود

$$\langle c, G(k) \oplus m \rangle,$$

که در آن، G یک مولد شبه تصادفی است. با داشتن یک متن رمز $\langle c, c' \rangle$، مهاجم می‌توان بیت آخر c' را وارون کند و یک متن رمز تغییریافته به دست آورد که یک رمزگذاری معتبر از m است که بیت آخر آن وارون شده است.

روش طبیعی برای رفع این مشکل عبارت است از استفاده از یک طرح رمزگذاری کلید خصوصی CCA-امن. ولی مشخص است که این امر کافی نیست اگر KEM در مقابل حملات متن رمز منتخب، آسیب‌پذیر باشد. ازآنجاکه هنوز این مفهوم را تعریف نکرده‌ایم، اکنون این کار را انجام می‌دهیم.

به‌مانند مفاد تعریف ۱۱-۱۱، ملزم می‌کنیم که یک متخاصم که یک متن رمز c را دریافت کرده است قادر به تمایز قائل شدن بین کلید k لفافه بندی شده توسط آن متن رمز از یک کلید k' یکنواخت و مستقل نباشد. بااین‌حال، اکنون همچنین به مهاجم اجازه می‌دهیم که لفافه زدایی متون رمز انتخابی خود را درخواست کند (مادامی‌که این متون رمز متفاوت از متن رمز چالش باشند).

به شکل رسمی، فرض کنید $\Pi = (Gen, Encaps, Decaps)$ یک KEM با طول کلید n و $\mathcal{A}$ یک متخاصم باشد و آزمایش زیر را در نظر بگیرید:

آزمایش تمایزناپذیری CCA؛ $KEM^{cca}_{\mathcal{A},\Pi}(n)$:

۱) $Gen(1^n)$ اجرا می‌شود تا کلیدهای (pk, sk) به دست آیند. آنگاه، $Encaps_{pk}(1^n)$ اجرا می‌شود تا (c,k) با $k \in \{0,1\}^n$ تولید شود.

۲) یک بیت $b \in \{0,1\}$ یکنواخت انتخاب می‌شود. اگر $b = 0$ باشد، قرار می‌دهیم $\hat{k} := k$ اگر $b = 1$ باشد، آنگاه یک $\hat{k} \in \{0,1\}^n$ یکنواخت را انتخاب می‌کنیم.

۳) مقادیر $(pk, c, \hat{k})$ و دسترسی به یک پیشگوی $Decaps_{sk}(\cdot)$ به $\mathcal{A}$ داده می‌شود ولی نمی‌تواند لفافه زدایی خود c را درخواست کند.

۴) $\mathcal{A}$ یک بیت b' را به‌عنوان خروجی ارائه می‌کند. خروجی آزمایش برابر با ۱ است اگر $b' = b$ و در غیر این صورت، برابر با ۰ خواهد بود.

تعریف ۱۱-۱۳

یک مکانیسم لفافه بندی کلید Π دارای امنیت CCA است اگر برای تمام متخاصمین زمان-چندجمله ای احتمالاتی $\mathcal{A}$، یک تابع ناچیز $negl$ وجود داشته باشد به صورتی که

$$\Pr[KEM^{cca}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + negl(n).$$

خوشبختانه، می‌توانیم نشان دهیم که استفاده از یک KEM دارای امنیت CCA همراه با یک طرح رمزگذاری کلید خصوصی CCA-امن منجر به یک طرح رمزگذاری کلید عمومی امن در برابر حملات متن رمز منتخب خواهد شد.

قضیه‌ی ۱۱-۱۴

اگر Π یک KEM دارای امنیت CCA باشد و Π' یک طرح رمزگذاری کلید خصوصی CCA-امن باشد، آنگاه Π^{hy} تعریف‌شده در ساختار ۱۱-۱۰، یک طرح رمزگذاری کلید عمومی CCA-امن است.

اثبات از طریق تغییر مناسب در اثبات قضیه‌ی ۱۱-۱۲ به دست می‌آید.

۱۱-۴- رمزگذاری مبتنی بر CDH/DDH

تاکنون رمزگذاری کلید عمومی را به‌صورت مجرد مورد بحث قرار داده‌ایم ولی هنوز هیچ مثال عینی از طرح‌های رمزگذاری کلید عمومی (یا KEMها) مشاهده نکرده‌ایم. در اینجا، تعدادی ساختار مبتنی بر مسائل دیفی-هلمن را بررسی می‌کنیم. (مسائل دیفی-هلمن در بخش ۸-۳-۲ معرفی شده‌اند.)

۱۱-۴-۱- رمزگذاری الجمال

در سال ۱۹۸۵، طاهر الجمال بیان نمود که پروتکل تبادل کلید دیفی-هلمن (ن.ک. بخش ۱۰-۳) را می‌توان تطبیق داد تا یک طرح رمزگذاری کلید عمومی به دست آید. یادآوری می‌کنیم که در پروتکل دیفی-هلمن، آلیس پیامی را برای باب ارسال می‌کند و سپس باب با یک پیام به آلیس، پاسخ می‌دهد؛ براساس این پیام‌ها، آلیس و باب می‌توانند یک مقدار تسهیمی k را به دست آورند که از یک عنصر یکنواخت از یک گروه مفروض $\mathbb{G}$ (برای یک شنودگر) تمایزناپذیر است. می‌توانیم تصور کنیم که باب از این مقدار تسهیمی برای رمزگذاری یک پیام $m \in \mathbb{G}$ با ارسال $k.m$ به آلیس، استفاده می‌کند؛ مشخص است که آلیس می‌تواند m را با استفاده از این امر که k را می‌داند، بازیابی کند و در ادامه استدلال می‌کنیم که شنودگر هیچ‌چیزی در مورد m نمی‌فهمد.

در طرح رمزگذاری الجمال، دیدگاه خود در خصوص تعامل بالا را تغییر می‌دهیم. ما، پیام اولیه‌ی آلیس را به‌عنوان کلید عمومی وی و پاسخ باب (هم پاسخ اولیه‌ی وی و هم $(k.m$) را به‌عنوان یک متن رمز در نظر می‌گیریم. امنیت CPA بر اساس فرض دیفی-هلمن تصمیمی (DDH) نسبتاً به‌سادگی از امنیت پروتکل تبادل کلید دیفی-هلمن (قضیه‌ی ۱۰-۳) نتیجه می‌شود.

در بررسی رسمی خود، با بیان و اثبات یک لم ساده آغاز می‌کنیم که اساس طرح رمزگذاری الجمال را شکل می‌دهد. فرض کنید $\mathbb{G}$ یک گروه متناهی باشد و $m \in \mathbb{G}$ را به‌عنوان یک عنصر دلخواه در نظر بگیرید. این لم بیان می‌کند که ضرب کردن m در یک عنصر گروهی یکنواخت y منجر به یک عنصر گروهی k' دارای توزیع یکنواخت خواهد شد. نکته‌ی مهم این است که این توزیع از k' مستقل از m است؛ این امر بدان معناست که k' شامل هیچ اطلاعاتی در مورد m نیست.

لم ۱۱-۱۵

فرض کنید $\mathbb{G}$ یک گروه متناهی و $m \in \mathbb{G}$ یک عنصر دلخواه باشد. آنگاه، انتخاب $k \in \mathbb{G}$ یکنواخت و قرار دادن $k' := k.m$ همان توزیعی را برای k' می‌دهد که انتخاب $k' \in \mathbb{G}$ یکنواخت، به دست خواهد داد. به‌بیان‌دیگر، برای هر $\hat{g} \in \mathbb{G}$، داریم

$$\Pr[k.m = \hat{g}] = 1/|\mathbb{G}|,$$

که در آن، احتمال بر روی انتخاب یکنواخت $k \in \mathbb{G}$ گرفته شده است.

اثبات

فرض کنید $\hat{g} \in \mathbb{G}$، دلخواه باشد. آنگاه

$$\Pr[k.m = \hat{g}] = \Pr[k = \hat{g}.m^{-1}].$$

ازآنجاکه k یکنواخت است، احتمال اینکه k برابر با عنصر ثابت $\hat{g}.m^{-1}$ باشد، دقیقاً برابر با $1/|\mathbb{G}|$ خواهد بود. ■

لم بالا روشی را برای ساختن یک طرح رمزگذاری کلید خصوصی کاملاً محرمانه با فضای پیام $\mathbb{G}$ می‌دهد. فرستنده و گیرنده به‌عنوان کلید رمز خود، یک عنصر یکنواخت $k \in \mathbb{G}$ را تسهیم می‌کنند. به‌منظور رمزگذاری پیام $m \in \mathbb{G}$، فرستنده، متن رمز $k' := k.m$ را محاسبه می‌کند. گیرنده می‌توان پیام را از متن رمز k' از طریق محاسبه‌ی $m := k'/k$ بازیابی کند. محرمانگی کامل به شکل فوری از لم بالا نتیجه می‌شود. درواقع، قبلاً این طرح را به شکلی متفاوت مشاهده کرده‌ایم- طرح رمزگذاری کلید یک‌بارمصرف یک نمونه از این رویکرد است، که گروه مبنای آن عبارت است از مجموعه رشته‌های با طول ثابت مفروض تحت عملیات XOR بیتی.

می‌توانیم ایده‌های بالا را به این صورت برای موقعیت کلید عمومی تطبیق دهیم که روشی برای تولید یک مقدار «شبه تصادفی» تسهیمی k از طریق تعامل بر روی یک کانال عمومی، به طرفین ارائه دهیم. این روش باید آشنا به نظر برسد چراکه دقیقاً همان چیزی است که پروتکل دیفی-هلمن فراهم می‌کند. جزئیات را در ادامه بیان می‌کنیم.

مثل بخش ۸-۲-۲، فرض کنید $\mathcal{G}$ یک الگوریتم زمان-چندجمله‌ای باشد که 1^n را به‌عنوان ورودی دریافت می‌کند و (مگر با احتمال ناچیز) توصیف یک گروه دوری $\mathbb{G}$، مرتبه‌ی آن، یعنی q (با $\|q\| = n$) و یک مولد g را به‌عنوان خروجی ارائه می‌کند. طرح رمزگذاری الجمال در ساختار ۱۱-۱۶ توصیف شده است.

طرح رمزگذاری الجمال

ساختار ۱۱-۱۶

فرض کنید $\mathcal{G}$ به شکل تعریف شده در متن باشد. یک طرح رمزگذاری کلید عمومی را به‌صورت زیر تعریف می‌کنیم:

- *Gen*: با دریافت 1^n به‌عنوان ورودی، $\mathcal{G}(1^n)$ را برای به دست آوردن $(\mathbb{G}, q, g)$ اجرا می‌کنیم. آنگاه یک $x \in \mathbb{Z}_q$ یکنواخت را انتخاب کرده و $h := g^x$ را محاسبه می‌کنیم. کلید عمومی برابر با $\langle \mathbb{G}, q, g, h \rangle$ و کلید خصوصی برابر با $\langle \mathbb{G}, q, g, x \rangle$ است. فضای پیام برابر با $\mathbb{G}$ است.
- *Enc*: با دریافت یک کلید عمومی $pk = \langle \mathbb{G}, q, g, h \rangle$ و یک پیام $m \in \mathbb{G}$ به‌عنوان ورودی، یک $y \in \mathbb{Z}_q$ یکنواخت را انتخاب کرده و متن رمز زیر را به‌عنوان خروجی ارائه می‌کنیم:
$$\langle g^y, h^y \cdot m \rangle$$
- *Dec*: با دریافت یک کلید خصوصی $sk = \langle \mathbb{G}, q, g, x \rangle$ و یک متن رمز $\langle c_1, c_2 \rangle$ به‌عنوان ورودی، خروجی زیر را ارائه می‌کنیم
$$\hat{m} := c_2/c_1^x$$

برای مشاهده‌ی اینکه رمزگشایی موفق می‌شود، فرض کنید $\langle c_1, c_2 \rangle = \langle g^y, h^y \cdot m \rangle$ با $h = g^x$ آنگاه

$$\hat{m} = \frac{c_2}{c_1^x} = \frac{h^y \cdot m}{(g^y)^x} = \frac{(g^x)^y \cdot m}{g^{xy}} = \frac{g^{xy} \cdot m}{g^{xy}} = m.$$

مثال ۱۱-۱۷

فرض کنید $q = 83$ و $p = 2q + 1 = 167$ و فرض کنید $\mathbb{G}$ نشان‌دهنده‌ی گروه مانده‌های درجه دوم به پیمانه‌ی p باشد. (ازآنجاکه p و q اول هستند، $\mathbb{G}$ یک زیرگروه از $\mathbb{Z}_p^*$ با مرتبه‌ی q است. ن.ک.

بخش ۸-۳-۳.) ازآنجاکه مرتبه‌ی $\mathbb{G}$، اول است، هر عنصر $\mathbb{G}$ به‌غیراز ۱، یک مولد است؛ قرار دهید $g = ۲^۲ = ۴ \bmod ۱۶۷$. فرض کنید گیرنده کلید رمز $x = ۳۷ \in \mathbb{Z}_{۸۳}$ را انتخاب می‌کند و بنابراین، کلید عمومی برابر است با

$$pk = \langle p, q, g, h \rangle = \langle ۱۶۷, ۸۳, ۴, [۴^{۳۷} \bmod ۱۶۷] \rangle = \langle ۱۶۷, ۸۳, ۴, ۷۶ \rangle,$$

که در آن، از p برای نمایش دادن $\mathbb{G}$ استفاده می‌کنیم (فرض بر آن است که گیرنده می‌داند که این گروه مجموعه‌ای از مانده‌های درجه دوم به پیمانه‌ی p است).

فرض کنید یک فرستنده، پیام $m = ۶۵ \in \mathbb{G}$ را رمزگذاری می‌کند (توجه کنید که $۶۵ = ۳۰^۲ \bmod ۱۶۷$ و بنابراین، ۶۵ یک عنصر در زیرگروه است). اگر $y = ۷۱$ باشد، متن رمز برابر است با

$$\langle [۴^{۷۱} \bmod ۱۶۷], [۷۶^{۷۱} \cdot ۶۵ \bmod ۱۶۷] \rangle = \langle ۱۳۲, ۴۴ \rangle.$$

برای رمزگشایی، گیرنده در ابتدا، $[۱۳۲^{۳۷} \bmod ۱۶۷] = ۱۲۴$ را محاسبه می‌کند، سپس، ازآنجاکه $[۱۲۴^{-۱} \bmod ۱۶۷] = ۶۶$ گیرنده $[۴۴ \cdot ۶۶ \bmod ۱۶۷] = ۶۵ = m$ را بازیابی می‌کند. ◊

اکنون، امنیت این طرح را اثبات می‌کنیم. (خواننده می‌تواند اثبات قضیه‌ی زیر را با اثبات‌های قضایای ۳-۱۸ و ۳-۱۰ مقایسه کند.)

قضیه‌ی ۱۱-۱۸

اگر مسئله‌ی DDH نسبت به $\mathcal{G}$ سخت باشد، آنگاه طرح رمزگذاری الجمال، CPA-امن است.

اثبات

فرض کنید Π نشان‌دهنده‌ی طرح رمزگذاری الجمال باشد. اثبات می‌کنیم که Π دارای رمزگذاری‌های تمایزناپذیر در حضور یک شنودگر است؛ بر اساس گزاره‌ی ۱۱-۳، این امر به شکل ضمنی نشان می‌دهد که این طرح، CPA-امن است.

فرض کنید $\mathcal{A}$ یک متخاصم زمان-چندجمله‌ای تصادفی باشد. می‌خواهیم نشان دهیم که یک تابع ناچیز $negl$ وجود دارد به صورتی که

$$\Pr[PubK^{eav}_{\mathcal{A},\Pi}(n) = ۱] \leq \frac{۱}{۲} + negl(n).$$

«طرح رمزگذاری» تغییریافته‌ی $\tilde{\Pi}$ را در نظر بگیرید که در آن، Gen مانند Gen در Π است ولی رمزگذاری یک پیام m نسبت به کلید عمومی $\langle \mathbb{G}, q, g, h \rangle$ با انتخاب $y, z \in \mathbb{Z}_q$ و ارائه‌ی متن رمز زیر به‌عنوان خروجی انجام می‌شود

$$\langle g^y, g^z \cdot m \rangle.$$

هرچند $\tilde{\Pi}$ درواقع یک طرح رمزگذاری نیست (چراکه هیچ راهی برای رمزگشایی در اختیار گیرنده نیست)، آزمایش $PubK^{eav}_{\mathcal{A},\tilde{\Pi}}(n)$ همچنان خوش‌تعریف است به این دلیل که این آزمایش تنها به الگوریتم‌های تولید کلید و رمزگذاری بستگی دارد.

لم ۱۱-۱۵ و بحثی که در ادامه‌ی آن آورده شده است به‌صورت ضمنی نشان می‌دهند که مؤلفه‌ی دوم متن رمز در طرح $\tilde{\Pi}$ عبارت است از یک عنصر گروهی دارای توزیع یکنواخت که علی‌الخصوص مستقل از پیام m مورد رمزگذاری است. (به یاد داشته باشید که g^z یک عنصر یکنواخت از $\mathbb{G}$ خواهد بود زمانی که z به‌صورت یکنواخت از $\mathbb{Z}_q$ انتخاب شده باشد.) اولین مؤلفه‌ی متن رمز به شکل بدیهی مستقل از m است. به همراه هم، این موارد به این معنا هستند که کل متن رمز شامل هیچ اطلاعاتی در مورد m نیست. نتیجه می‌گیریم که

$$\Pr[PubK^{eav}_{\mathcal{A},\tilde{\Pi}}(n) = ۱] = \frac{۱}{۲}.$$

اکنون الگوریتم PPT زیر، یعنی D، را در نظر بگیرید که تلاش می‌کند تا مسئله‌ی DDH را نسبت به $\mathcal{G}$ حل کند. یادآوری می‌کنیم که D مقادیر $\langle \mathbb{G}, q, g, h_۱, h_۲, h_۳ \rangle$ را دریافت می‌کند که در آن، $h_۱ = g^x$ و $h_۲ = g^y$ و $h_۳$ یا برابر با g^{xy} یا g^z (برای x, y, z یکنواخت) است؛ هدف D عبارت است از تعیین اینکه کدام حالت صدق می‌کند.

الگوریتم D

این الگوریتم، مقادیر $\langle \mathbb{G}, q, g, h_۱, h_۲, h_۳ \rangle$ را به‌عنوان ورودی دریافت می‌کند.

- قرار می‌دهیم $pk = \langle \mathbb{G}, q, g, h_۱ \rangle$ و $\mathcal{A}(pk)$ را اجرا می‌کنیم تا دو پیام $m_۰, m_۱ \in \mathbb{G}$ را به دست آوریم.
- یک بیت یکنواخت b را انتخاب کرده و قرار می‌دهیم $c_۱ := h_۲$ و $c_۲ := h_۳ \cdot m_b$.
- متن رمز $\langle c_۱, c_۲ \rangle$ را به $\mathcal{A}$ داده و یک بیت خروجی b' را به دست می‌آوریم. اگر $b' = b$ باشد، خروجی ۱ را ارائه می‌کنیم؛ در غیر این صورت، خروجی ۰ را ارائه می‌کنیم.

اجازه دهید رفتار D را تحلیل کنیم. دو حالت را باید مدنظر قرار دهیم:

حالت اول

فرض کنید ورودی برای D با اجرای $\mathcal{G}(۱^n)$ برای به دست آوردن $\langle \mathbb{G}, q, g \rangle$، سپس انتخاب $x, y, z \in \mathbb{Z}_q$ یکنواخت و درنهایت قرار دادن $h_۱ := g^x$ و $h_۲ := g^y$ و $h_۳ := g^z$ تولید می‌شود. سپس، D، $\mathcal{A}$ را بر روی یک کلید عمومی ساخته‌شده به‌صورت

$$pk = \langle \mathbb{G}, q, g, g^x \rangle$$

و یک متن رمز ساخته‌شده به‌صورت $\langle c_۱, c_۲ \rangle = \langle g^y, g^z \cdot m_b \rangle$ اجرا می‌کند. مشاهده می‌کنیم که در این حالت، دیدگاه $\mathcal{A}$ هنگام اجراشدن به‌عنوان یک زیرروال توسط D دارای توزیع یکسان با دیدگاه

$\mathcal{A}$ در آزمایش $PubK^{eav}_{\mathcal{A},\Pi}(n)$ است. ازآنجاکه D دقیقاً زمانی خروجی ۱ را ارائه می‌کند که خروجی b' ارائه‌شده توسط $\mathcal{A}$ برابر با b باشد، داریم

$$\Pr[D(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] = \Pr[PubK^{eav}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2}.$$

حالت دوم

فرض کنید ورودی برای D با اجرای $\mathcal{G}(1^n)$ برای به دست آوردن $(\mathbb{G}, q, g)$، سپس انتخاب $x, y \in \mathbb{Z}_q$ یکنواخت و درنهایت قرار دادن $h_1 := g^x$، $h_2 := g^y$ و $h_3 := g^{xy}$ تولید می‌شود. آنگاه، D، $\mathcal{A}$ را بر روی یک کلید عمومی ساخته شده به‌صورت

$$pk = \langle \mathbb{G}, q, g, g^x \rangle$$

و یک متن رمز ساخته‌شده به‌صورت

$$\langle c_1, c_2 \rangle = \langle g^y, g^{xy} \cdot m_b \rangle = \langle g^y, (g^x)^y \cdot m_b \rangle$$

اجرا می‌کند. مشاهده می‌کنیم که در این حالت، دیدگاه $\mathcal{A}$ هنگام اجراشدن به‌عنوان یک زیرروال توسط D دارای توزیع برابر با دیدگاه $\mathcal{A}$ در آزمایش $PubK^{eav}_{\mathcal{A},\Pi}(n)$ خواهد بود. ازآنجاکه D خروجی ۱ را دقیقاً زمانی ارائه می‌کند که b' خروجی از $\mathcal{A}$ برابر با b باشد، داریم

$$\Pr[D(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1] = \Pr[PubK^{eav}_{\mathcal{A},\Pi}(n) = 1].$$

تحت این فرض که مسئله‌ی DDH نسبت به $\mathcal{G}$ سخت است، یک تابع ناچیز $negl$ وجود دارد به صورتی که

$$\begin{aligned} Negl(n) &\geq \left|\Pr[D(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] - \Pr[D(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1]\right| \\ &= \left|\frac{1}{2} - \Pr[PubK^{eav}_{\mathcal{A},\Pi}(n) = 1]\right|. \end{aligned}$$

این نتیجه به شکل ضمنی نشان می‌دهد که $\Pr[PubK^{eav}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$، که اثبات را کامل می‌کند. ■

مشکلات پیاده‌سازی الجمال

تعدادی از مشکلات عملی مربوط به رمزگذاری الجمال را به‌صورت مختصر بررسی می‌کنیم.

تسهیم پارامترهای عمومی

توصیف ما برای طرح رمزگذاری الجمال در ساختار ۱۱-۱۶ گیرنده را ملزم می‌کند تا $\mathcal{G}$ را برای تولید $\mathbb{G}, q, g$ اجرا نماید. در عمل، معمولاً این پارامترها «یک‌بار برای همیشه» تولید و مشخص می‌شوند و سپس در میان چندین گیرنده، تسهیم می‌شوند. (البته هر گیرنده باید مقدار رمز x مختص خود را

برخاب کرده و کلید عمومی مختص خود، $h = g^x$ را منتشر نماید.) برای مثال، $NIST$ مجموعه‌ای از پارامترهای پیشنهادی مناسب برای استفاده در طرح رمزگذاری الجمال را منتشر کرده است. تسهیم پارامترها به این شیوه تأثیری بر امنیت نخواهد داشت (با این فرض که پارامترها به‌درستی و به شکل صادقانه تولید شده باشند). با نگاهی به آینده، بیان می‌کنیم که این شیوه در تضاد با حالت RSA است که در آن، پارامترها را نمی‌توان به شکل امن، تسهیم نمود (ن.ک. بخش ۱۱-۵-۱).

انتخاب گروه

همان‌طور که در بخش ۸-۳-۲ بحث شد، مرتبه‌ی گروه q معمولاً به‌صورت یک عدد اول انتخاب می‌شود. تا آنجایی که مسئله‌ی گروه‌های خاص مطرح است، خم‌های بیضوی یک گزینه‌ی محبوب هستند؛ یک جایگزین برای این خم‌ها این است که $\mathbb{G}$ را یک زیرگروه مرتبه اول از $\mathbb{Z}_p^*$ برای p اول، در نظر بگیریم. برای مشاهده‌ی جدولی از طول کلیدهای پیشنهادی برای رسیدن به سطوح امنیت متفاوت می‌توانید به بخش ۹-۳ مراجعه کنید.

فضای پیام

یک بعد دشوار از طرح رمزگذاری الجمال آن است که فضای پیام یک گروه $\mathbb{G}$ است و نه رشته‌های بیتی با یک طول خاص مفروض. برای بعضی انتخاب‌های گروه، امکان حل این مسئله با تعریف یک کدگذاری وارون‌پذیر از رشته‌های بیتی به‌عنوان اعضای گروه وجود دارد. در چنین مواردی، فرستنده در ابتدا می‌تواند پیام $m \in \{0,1\}^\ell$ خود را به‌عنوان یک عنصر گروهی $\widehat{m} \in \mathbb{G}$ کدگذاری نموده و سپس رمزگذاری الجمال را بر روی $\widehat{m}$ اعمال نماید. گیرنده می‌تواند رمزگشایی را به شکل بیان‌شده در ساختار ۱۱-۱۶ به‌منظور به دست آوردن پیام کدگذاری شده‌ی $\widehat{m}$ انجام دهد و سپس کدگذاری را وارون نماید تا پیام اولیه‌ی m به دست آید.

یک رویکرد ساده‌تر عبارت است از استفاده از (یک‌گونه از) رمزگذاری الجمال به‌عنوان بخشی از یک طرح رمزگذاری ترکیبی. برای مثال، فرستنده می‌تواند یک عنصر گروهی $m \in \mathbb{G}$ یکنواخت را انتخاب نماید، این عنصر را با استفاده از طرح رمزگذاری الجمال، رمزگذاری کند و سپس پیام واقعی خود را با استفاده از یک طرح رمزگذاری کلید خصوصی و کلید $H(m)$ رمزگذاری نماید که در آن، $H: \mathbb{G} \to \{0,1\}^\ell$ یک تابع برگرفتن کلید مناسب (ن.ک. بخش بعدی) است. در این حالت، استفاده از KEM مبتنی بر DDH کارایی بیشتری خواهد داشت که در ادامه آن را توصیف می‌کنیم.

۱۱-۴-۲- لفافه بندی کلید مبتنی بر DDH

در انتهای بخش قبلی اشاره کردیم که رمزگذاری الجمال را می‌توان به‌عنوان بخشی از یک طرح رمزگذاری ترکیبی به این صورت مورد استفاده قرار داد که یک عنصر گروهی یکنواخت m را با استفاده از یک چکیده‌سازی از آن عنصر به‌عنوان یک کلید، رمزگذاری نماییم. ولی این شیوه باعث

هدر رفت منابع می‌شود! اثبات امنیت برای رمزگذاری الجمال نشان می‌دهد که c_0^x (که در آن، c_0 اولین مؤلفه‌ی متن رمز و x کلید خصوصی گیرنده است) اکنون هم از یک عنصر گروهی یکنواخت تمایزناپذیر است، بنابراین فرستنده/گیرنده می‌تواند از همان استفاده کند. ساختار ۱۱-۱۹ نشان‌دهنده‌ی KEM است که از این رویکرد تبعیت می‌کند. توجه کنید که لفافه بندی به‌دست‌آمده شامل تنها یک عنصر گروهی یکتا است. در مقابل، اگر قرار باشد از رمزگذاری الجمال یک عنصر گروهی یکنواخت استفاده کنیم، متن رمز شامل دو عنصر گروهی خواهد بود.

یک KEM «شبه الجمال»

ساختار ۱۱-۱۹

فرض کنید $\mathcal{G}$ به شکل تعریف شده در بخش قبلی باشد. یک KEM را به شکل زیر تعریف کنید:

- Gen: با دریافت 1^n به‌عنوان ورودی، $\mathcal{G}(1^n)$ را اجرا می‌کنیم تا $(\mathbb{G}, q, g)$ به دست آید. یک $x \in \mathbb{Z}_q$ یکنواخت را انتخاب کرده و قرار می‌دهیم $h := g^x$. همچنین یک تابع $H: \mathbb{G} \to \{0,1\}^{\ell(n)}$ برای یک تابع مفروض l (ن.ک. متن) را مشخص می‌کنیم. کلید عمومی برابر با $\langle \mathbb{G}, q, g, h, H \rangle$ و کلید خصوصی برابر با $\langle \mathbb{G}, q, g, x \rangle$ است.
- $Encaps$: با دریافت یک کلید عمومی $pk = \langle \mathbb{G}, q, g, h, H \rangle$ به‌عنوان ورودی، یک $y \in \mathbb{Z}_q$ یکنواخت را انتخاب می‌کنیم و متن رمز g^y و کلید $H(h^y)$ را به‌عنوان خروجی ارائه می‌کنیم.
- $Decaps$: با دریافت یک کلید خصوصی $sk = \langle \mathbb{G}, q, g, x \rangle$ و یک متن رمز $c \in \mathbb{G}$ به‌عنوان ورودی، کلید $H(c^x)$ را به‌عنوان خروجی ارائه می‌کنیم.

همان‌طور که تبیین شد، این ساختار، تابع برگرفتن کلید H را مشخص نمی‌کند و چندین گزینه برای این تابع وجود دارد. (برای اطلاعات بیشتر در خصوص برگرفتن کلید به‌طورکلی ن.ک. بخش ۵-۶-۴.) یک گزینه عبارت است از انتخاب یک تابع $H: \mathbb{G} \to \{0,1\}^\ell$ که (نزدیک به) «منتظم» باشد، به این معنا که برای هر کلید ممکن $k \in \{0,1\}^\ell$، تعداد اعضای گروه که به k نگاشت می‌شوند تقریباً یکسان است. (به شکل رسمی، نیازمند یک تابع ناچیز $negl$ هستیم به صورتی که برای هر $k \in \{0,1\}^\ell$ داشته باشیم

$$\left| \Pr[H(g) = k] - 2^{-\ell} \right| \leq \mathrm{negl}(n),$$

که در آن، احتمال روی انتخاب یکنواخت $g \in \mathbb{G}$ گرفته شده است. این امر تضمین می‌کند که توزیع بر روی کلید k ازلحاظ آماری نزدیک به یکنواخت باشد.) هم پیچیدگی H و هم طول کلید قابل‌دستیابی l به گروه خاص $\mathbb{G}$ استفاده‌شده، بستگی خواهد داشت.

یک گزینه‌ی دیگر این است که H را یک تابع «کلیددار» در نظر بگیریم که در آن، کلید (یکنواخت) برای H به‌عنوان بخشی از کلید عمومی گیرنده در نظر گرفته می‌شود. این شیوه مفید است اگر H یک استخراج‌کننده‌ی قوی باشد، همان‌طور که به شکل مختصر در بخش ۵-۶-۴ اشاره شد. انتخاب

درست l در اینجا (برای تضمین اینکه کلید به‌دست‌آمده ازلحاظ آماری نزدیک به یکنواخت خواهد بود) به‌اندازه‌ی $\mathbb{G}$ بستگی خواهد داشت.

در هرکدام از حالات بالا، اثبات CPA-امن بودن بر اساس فرض دیفی-هلمن تصمیمی (DDH) به‌سادگی با تطبیق اثبات امنیت برای پروتکل تبادل کلید دیفی-هلمن (قضیه‌ی ۱۰-۳) نتیجه می‌شود.

قضیه‌ی ۱۱-۲۰

اگر مسئله‌ی DDH نسبت به $\mathcal{G}$ سخت باشد و H به‌صورت توصیف شده انتخاب شده باشد، آنگاه ساختار ۱۱-۱۹ یک KEM دارای امنیت CPA خواهد بود.

اگر مایل به مدل‌سازی H به‌عنوان یک «پیشگوی تصادفی» باشیم، آنگاه CPA-امن بودن ساختار ۱۱-۱۹ را می‌توان بر اساس فرض (ضعیف‌تر) دیفی-هلمن محاسباتی (CDH) اثبات نمود. این مقوله را در بخش بعدی مورد بحث قرار می‌دهیم.

۱۱-۴-۲-۵ یک KEM مبتنی بر CDH در مدل پیشگوی تصادفی

در این بخش، نشان می‌دهیم که اگر مایل به مدل‌سازی H به‌عنوان یک «پیشگوی تصادفی» باشیم، آنگاه CPA-امن بودن ساختار ۱۱-۱۹ را می‌توان بر اساس فرض CDH اثبات نمود. (خوانندگان می‌توانند بخش ۵-۵ را مرور کنند تا مدل پیشگوی تصادفی برای آن‌ها یادآوری شود.) به شکل شهودی، فرض CDH نشان می‌دهد که مهاجم مشاهده‌کننده‌ی $h = g^x$ (از روی کلید عمومی) و متن رمز $c = g^y$ نمی‌تواند $\mathrm{DH}_g(h, c) = h^y$ را محاسبه کند. علی‌الخصوص، آنگاه، مهاجم نمی‌تواند h^y را از پیشگوی تصادفی، پرسمان کند. ولی این امر به این معنا است که کلید لفافه بندی شده‌ی $H(h^y)$ از دیدگاه مهاجم، کاملاً تصادفی است. این برداشت شهودی در ادامه به یک اثبات رسمی بدل می‌شود.

همان‌طور که برداشت شهودی بالا نشان می‌دهد، اثبات به‌صورت ذاتی به مدل‌سازی H به‌عنوان یک پیشگوی تصادفی تکیه می‌کند[۲۳]. علی‌الخصوص، این اثبات به این واقعیت‌ها تکیه دارد که (۱) تنها شیوه برای فهمیدن $H(h^y)$ پرسمان h^y به شکل آشکار از H است که به این معنا خواهد بود که مهاجم یک نمونه CDH را حل کرده است (این مقوله در بخش ۵-۵-۱، «استخراج پذیری» نامیده می‌شود) و (۲) اگر مهاجم h^y را از H پرسمان نکند، آنگاه مقدار $H(h^y)$ از دیدگاه مهاجم، یکنواخت

[۲۳] این امر صدق می‌کند مادامی‌که بخواهیم تنها به فرض CDH تکیه کنیم. همان‌طور که قبلاً اشاره شد، یک اثبات بدون پیشگوهای تصادفی، امکان‌پذیر خواهد بود اگر ما بر فرض قوی‌تر DDH تکیه کنیم.