سیستم رمز کلید عمومی McEliece امن معنایی - تبدیلات برای McEliece PKC

چکیده

تقریباً تمامی سیستم های رمز کلید-عمومی کنونی (PKCها) بر اساس تئوری اعداد، مانند مسئله فاکتوربندی عدد صحیح و مسئله لگاریتم گسسته هستند (که در چندجمله ای-زمانی بعد از ظهور کامپیوترهای کوانتوم حل خواهد شد). در حالیکه McEliece PKC بر اساس تئوری دیگری است، یعنی تئوری کدگذاری، در مقابل چندین حمله عملی مستعد است. در این مقاله، ما به دقت حملات کنونی شناخته شده برای McEliece PKC را بازنگری می کنیم و سپس نشان می دهیم که بدون هر پیشگویی آشکارسازی یا هر دانش جزئی در مورد پیام عادی مهنادار پیام رمزی چالش، هیچ الگوریتم زمانی چندجمله ای برای تبدیل McEliece PKC وجود ندارد که پارامترهای آن به دقت انتخاب شده باشند. تحت این فرض که این مسئله تبدیل سخت است، ما به طور مختصر نسخه های اصلاح شده McEliece PKC را پیشنهاد می دهیم که می تواند در مدل پیشگویی تصادفی که باید به طور معنادار در مقابل حملات پیام متنی-انتخاب شده تطبیقی امن شود، اثبات شود. تبدیلات ما می تواند کاهش داده های افزونه را به 1/3 ~ 1/4 در مقایسه با تبدیلات ذاتی برای پارامترهای عملی حاصل نماید.

1 مقدمه

از زمانی که مفهوم سیستم رمز کلید عمومی (PKC) توسط Diffie and Hellman [5], مطرح شد، بسیاری از محققان PKCهای متعددی را بر اساس مسائل مختلف، مانند فاکتوربندی عدد صحیح، لگاریتم گسسته، کدگشایی کد خطی بزرگ، کوله پشتی، تبدیل معادلات چندجمله ای و غیره پیشنهاد نمودند. در حالیکه برخی از آنها هنوز حاضر هستند، بیشتر آنها توسط رمزنویس به علت تحلیل رمز شدید شکسته شدند. به عنوان نتیجه، تقریباً تمامی سیستم های امن کنونی، فقط یک کلاس کوچک از PKCها، مانند RSA و سیستم های رمز منحنی بیضوی را به کار

می گیرند که همه بر اساس مسئله فاکتوربندی عدد صحیح (IFP) یا مسئله لگاریتم گسسته (DLP) هستند. این وضعیت سبب مسئله ای جدی می شود بعد از اینکه کسی یک الگوریتم عملی را کشف کند که IFP و DLP را به چند جمله ای-زمانی بشکند. هیچ کس نمی تواند بگوید که چنین الگوریتمی هرگز یافت نشود. واقعاً، Shor قبلاً یک الگوریتم (احتمالی) چندجمله ای-زمانی را در [25] کشف نموده است، حتی اگر نیاز به کامپیوتر کوانتوم داشته باشد که تا به حال غیرعملی بوده است. به منظور آماده سازی برای آن وضعیت تاسف بار، ما نیاز به یافتن نقشه امن دیگری داریم که روی IFP و DLP تکیه می کند.

McEliece PKC که توسط R.J McElice در [18] پیشنهاد شده است، یکی از جایگزین های معدود برای PKCهای مبتنی بر IFP یا DLP است. این مورد مبتنی بر مسئله کدگشایی کد خطی بزرگ بدون هیچ ساختار مرئی است که به عنوان یک مسئله کامل-NP حدس زده می شود. در حالیکه هیچ الگوریتم زمانی-چندجمله ای تا کنون برای کدگشایی یک کد خطی دلخواه با طول بزرگ بدون ساختار مرئی کشف نشده است، بسیاری از حملات (برخی از آنها در چندجمله ای-زمانی کار می کنند) برای McEliece PKC شناخته شده اند [1,3,4,12,15,28,17,13].

در این مقاله ما به دقت این حملات را در بخش [3] بازنگری می کنیم و سپس نشان می دهیم که تمام حملات جمله ای زمانی به McEliece PKC نیاز به پیشگویی ها رمزگشایی یا دانش جزئی در مورد متن مهنادار متناظر متن رمزی چالش دارد. و در نتیجه بدون آنها، حمله جمله ای-زمانی برای تبدیل McEliece PKC شناخته شده است (که پارامترهای آن به دقت انتخاب می شوند). تحت این فرض که این مسئله تبدیل سخت است، ما این مسئله را به McEliece PKC معنادار امن در مقابل حملات متن رمزی-انتخاب شده تطبیقی (CCA2) تبدیل می کنیم، با معرفی برخی از تبدیلات مناسب. ما بررسی می کنیم که تبدیلات برای McEliece PKC در بخش [4] متناسب هستند. در حالیکه برخی از تبدیلات عام پیشنهاد شده در [24,9] نیز برای McEliece PKC قابل کاربرد هستند، آنها دارای عیبی در افزونگی داده ها هستند (که توسط اختلاف بین اندازه متن رمزی و اندازه متن مهنادار تعریف می

شود). میزان زیادی از داده های افزونه برای تبدیلات عام نیاز می شود زیرا اندازه بلوک McEliece PKC نسبتاً بزرگ است. تبدیلات ما در بخش 4.4 نیاز به داده های افزونه کمتری نسبت به موارد عام دارند.

2 سیستم های رمز کلید عمومی McEliece

در این بخش، ما به طور مختصر McEliece PKC را توصیف می کنیم.

تولید کلید: سه ماتریس کلید G,S,P زیر را ایجاد کنید:

G= k*n ماتریس تولیدکننده یک کد Goppa دودویی که می تواند t خطا را تصحیح نماید و برای آن یک الگوریتم کدگشایی کارامد شناخته شده است. پارامتر t توسط $\left\lceil \frac{d_{min}-1}{2} \right\rceil$ ارائه می شود که در ان dmin مینیمم فاصله Hamming برای کد است.

S: ماتریس غیرتکین دودویی تصادفی

P: ماتریس جایگشت تصادفی

آنگاه، ماتریس k*n، G'=SGP را محاسبه کنید.

کلید رمز : (S,G,P)

کلید عمومی: (G',t)

پنهان کردن: متن رمزی c برای یک پیام m به صورت زیر محاسبه می شود:

$$c = mG' \oplus z \qquad (1)$$

که در ان m در برداری دودویی با طول k نشان داده می شود و z نشاندهنده بردار خطای دودویی تصادفی با طول n و دارای t 1ام است.

کشف رمز: ابتدا: cP^{-1} را محاسبه کنید.

$$cP^{-1} = (mS)G \oplus zP^{-1} \qquad (2)$$

که در آن P^{-1} نشاندهنده معکوس P است. دوم، الگوریتم کدگشایی EC را برای G تا cP^{-1} اعمال کنید.

چون وزن Hamming برای zP^{-1} t است، می تواند mS را به دست آورد

$$mS = \mathrm{EC}(cP^{-1}). \qquad (3)$$

متن مهنادار رمزی c عبارتست از

$$m = (mS)S^{-1}. \qquad (4)$$

3 حملات به McEliece PKC

در این بخش، ما حملات کنونی شناخته شده به McEliece PKC را بازنگری می کنیم.

در حالیکه هیچ الگوریتم کارامدی تاکنون برای تجزیه G’ به (S,G,P) [19] کشف نشده است، حمله ساختاری در [17] کشف شده است. این حمله بخشی از ساختار G’ ضعیف را نشان می دهد که از چندجمله ای Goppa دودویی ایجاد می شود. هرچند، از این حمله می توان به سادگی با اجتناب از استفاده از کلیدهای عمومی ضعیف اجتناب نمود. (این نشان می دهد که G نباید یک کد BCH باشد از اینرو معادل کد Goppa است که چندجمله ای Goppa آن $1 \cdot x^{2t}$ یعنی دودویی است). مورد بعدی که باید در نظر بگیریم اینست که یک کد Goppa معادل برای G’ (که لزوماً G نیست) و الگوریتم کدگشایی آن شناخته شده است اتفاق می افتد. این احتمال در [1.10] تخمین زده می شود و آنگاه کوچک و قابل چشمپوشی نشان داده می شود.

تمام حملات دیگر شناخته شده برای رمزگشایی متون رمزی بدون شکستن کلیدهای عمومی هستند. ما آنها را به دو رده زیر، حملات بحرانی و حملات غیربحرانی مطابق با اینکه آیا این حملات می توانند به سادگی با بزرگ نمودن اندازه پارامتر اجتناب شوند یا خیر، رده بندی می کنیم. اگر اجتناب صورت گیرد، ما آن را در حملات غیربحرانی رده بندی می کنیم. در غیراینصورت، در موارد بحرانی. از آن جالب تر، تمام حملات بحرانی نیاز به اطلاعات اضافی دارند،

مانند دانش جزئی در مورد متون مهنادار هدف یا پیشگویی رمزگشایی که می تواند به طور دلخواه متون رمزی را به جز متون رمزی چالش رمزگشایی نماید. و آنگاه بدون این اطلاعات اضافی و این قابلیت، هیچ الگوریتم کارامدی برای رمزگشایی متن رمزی معین دلخواه برای McEliece PKC شناخته شده نیست.

3.1 حملات غیربحرانی

دو حمله زیر می تواند به سادگی با بزرگ نمودن اندازه پارامتر یا با اعمال اصلاح Loidreau [16] بدون بزرگ نمایی اندازه پارامتر اجتناب شود. بنابراین غیربحرانی است.

حمله کدگشایی-مجموعه-اطلاعات عمومی. در نظر بگیرید که $G'_k,\ c_k \text{ and } z_k$ نشاندهنده k ستون برداشته شده از G'، c و z به ترتیب باشد. آنها رابطه زیر را دارند

$$c_k = mG'_k \oplus z_k. \qquad (5)$$

اگر zk=0 و G'k غیرتکین باشد،m می تواند با [1] بازیابی شود

$$m = c_k G'^{-1}_k. \qquad (6)$$

حتی اگر $z_k \neq 0$ ، m می تواند با حدس زدن zk در میان تمام وزن های Hamming کوچک [15] بازیابی شود (ما این مورد را حمله کدگشایی-مجموعه-اطلاعات عمومی (GISD) می نامیم). صحت متن مهنادار بازیابی شده m با کنترل این مورد قابل تایید است که آیا وزن Hamming $c \oplus mG'$ است یا خیر.

هزینه محاسباتی این نسخه عمومی (که در آن zk حدس زده می شود) به طور مختصر سریع تر از موردی اصلی است (که در آن zk صفر فرض می شود)، اما هنوز برای پارامترهای مناسب غیرعملی است از اینرو هزینه محاسباتی آن به طور مجانبی با $C(n,k)/C(n-t,k).$ محدود می شود.

حمله یافتن-کلمه کد-وزن-کم. این حمله از یک الگوریتم استفاده می کند که کلمه کد با وزن کم را در میان کلمه کدهای تولید شده توسط ماتریس تولیدکننده دلخواه با استفاده از پایگاه داده به دست آمده توسط پیش محاسبه می یابد [26,4]، به علت کلمه کد وزن مینیمم ماتریس تولیدکننده (K+1)*n

$$\begin{bmatrix} G' \\ c \end{bmatrix} \qquad (7)$$

بردار خطای z از c است که در آن $c = mG' \oplus z$. ، این الگوریتم می تواند برای بازیابی m از متن رمزی داده شده c استفاده شود.

هزینه محاسباتی دقیق این حمله در [4] ارزیابی می شود و بنابراین برای غیرعملی بودن تبدیل c برای پارامترهای مناسب نشان داده می شود مثلاً $n \geq 2048$، و k و t بهینه سازی می شود حتی اگر پارامترهای اصلی $(n, k, t) = (1024, 524, 50)$ پیشنهاد شده در [18] با فاکتور کاری $2^{64.2}$ غیرعملی باشد (تحت این فرض که هر تکرار مستقل باشد، هزینه محاسباتی مورد انتظار برای این حمله به طور مجانبی کمتر توسط $C(n, k+1)/C(n-t, k+1)$ محدود شود و بنابراین برای پارامترهای مناسب غیرعملی است).

3.2 حملات بحرانی

از حملات زیر نمی توان توسط بزرگنمایی اندازه پارامتر یا با اعمال اصلاح Loidreau اجتناب نمود [16]. بنابراین بحرانی است.

حمله متن مهنادار-جزئی-شناخته شده. دانش جزئی در مورد متن مهنادار، هزینه محاسباتی حملات به McEliece PKC کاهش می دهد [4,13].

برای مثال، در نظر بگیرید که ml و mr نشاندهنده بیت های چپ و kr بیت های باقیمانده در متن مهنادار هدف m باشد، یعنی $k = k_l + k_r \text{ and } m = (m_l||m_r)$ ، فرض کنید که حریف mr را می داند. بنابراین، مشکل بازیابی متن مهنادار مجهول ml در McEliece PKC با پارامترهای (n,k) معادل بازیابی متن مهنادار کامل در McEliece PKC با پارامترهای (n,kl) است بنابراین

$$\begin{aligned} c &= mG' \oplus z \\ c &= m_l G'_l \oplus m_r G'_r \oplus z \\ c \oplus m_r G'_r &= m_l G'_l \oplus z \\ c' &= m_l G'_l \oplus z, \end{aligned} \tag{8}$$

که در آن G'l و G'r سطرهای بالایی kl و kr سطرهای پایینی باقیمانده در G' به ترتیب می باشند.

اگر kl در مقداری کوچک تثبیت شود، هزینه محاسباتی بازیابی بیت های kl مجهول از c، و G' چندجمله ای n است زیرا حتی اگر حملات غیربحرانی استفاده شوند، به طور مجانبی توسط $k_l^3 C(n, k_l)/C(n-t, k_l)$ محدود می شود که در آن kl ثابتی کوچک است.

حمله پیام-مرتبط. این حمله از دانش در مورد رابطه بین متون مهنادار هدف استفاده می کند [3].

فرض کنید که دو پیام m1 و m2 در c1 و c2 رمزگذاری شوند که در آن $c_1 = m_1 G' \oplus z_1,\ c_2 = m_2 G' \oplus z_2, \text{ and } z_1 \neq z_2$. اگر حریف رابطه خطی آنها را بین متون مهنادار بداند، مثلاً $\delta m = m_1 \oplus m_2$. آنگاه حریف می تواند به طور کارامد حمله GISD را به c1 و c2 با انتخاب مختصات k اعمال نماید که مقادیر آن 0 در $(\delta m G' \oplus c_1 \oplus c_2)$ هستند. از اینرو $z_1 \oplus z_2 = \delta m G' \oplus c_1 \oplus c_2$ و وزن t Hamming برای بردار خطای z بسیار کمتر از n/2 است. بنابراین یک مختصات در $(\delta m G' \oplus c_1 \oplus c_2)$ باید در z1 و z2 با احتمال بالا 0 باشد

زمانی که همان پیام دوبار (یا بیشتر) با استفاده از بردارهای خطای مختلف z1 و z2 رمزگذاری شود، مقدار $z_1 \oplus z_2$ به سادگی با $c_1 \oplus c_2$. نشان داده می شود. این مورد به عنوان حمله پیام-دوباره فرستاده شده ارجاع می شود [3].

حمله واکنش. این حمله می تواند به صورت حمله متن رمزی-انتخاب شده (CCA) رده بندی شود، اما از فرضی ضعیف تر از CCA استفاده می کند [12]: حریف تنها واکنش دریافت کننده ای را مشاهده می کند که دارای کلید خصوصی است، اما نیاز به دریافت متن مهنادار رمزگشایی شده آن ندارد (حمله مشابه به طور مستقل در [28] پیشنهاد می شود). در این حمله، یک حریف، متون مهنادار متناظر را دریافت می کند. بنابراین این حمله به صورت CCA رده بندی می شود.

ایده این حمله به صورت زیر است. حریف یک یا چند بیت از متن رمزی هدف c را برعکس می کند. در نظر بگیرید که c′ نشاندهنده متن رمزی برعکس شده باشد. حریف c′ را به دریافت کننده مناسب انتقال می دهد و واکنش او را مشاهده می کند. واکنش های گیرنده می تواند به دو رده تقسیم شود:

واکنش A: به علت خطای غیرقابل تصحیح یا به علت متن مهنادار بدون معنی، درخواست تکرار را به حریف بازگردانید.

واکنش B: یک تشکر را بازگردانید یا هیچ کاری انجام ندهید زیرا متن مهنادار مناسب m رمزگشایی شده است.

اگر وزن کلی بردار خطا از t بعد از برعکس نمودن تجاوز نکند، واکنش B مشاهده می شود. در غیراینصورت واکنش A مشاهده می شود. بنابراین با تکرار مشاهدات بالا، زمان های چندجمله ای n، حریف می تواند بردار خطا را تعیین کند. زمانی که بردار خطا تعیین شود، متن مهنادار متناظر به اسانی با استفاده از حمله GISD رمزگشایی می شود.

حمله قابلیت انعطاف. این حمله حریف را برای عوض کردن هر بخش از متن مهنادار متناظر برای هر متن رمزی داده شده c بدون شناختن متن مهنادار m مجاز می سازد، یعنی حریف می تواند یک متن رمزی جدید c′ را تولید کند که متن مهنادار آن $m \oplus \delta m$ از هر متن رمزی معین بدون شناختن m است [13,28].

این حمله به صورت زیر توصیف می شود. در نظر بگیرید که G′[i] نشاندهنده سطر iام ماتریس عمومی G′ و $I = \{i_1, i_2, \cdots\}$ نشاندهنده مجموعه ای از مختصات ij باشد که مقدار ان در δm 1 است. متن رمزی c′ به صورت زیر محاسبه می شود

$$c' = c \bigoplus_{i \in I} G'[i] = (m \oplus \delta m)G' \oplus z = m'G' \oplus z. \qquad (9)$$

این حمله به ما می گوید که McEliece PKC غیرانعطاف پذیر بودن را برآورده نمی سازد [6]. حتی در مقابل حملات مجهول، مانند حملات متن مهنادار انتخاب شده. و بنابراین تحت سناریوی متن رمزی انتخاب شده که در آن یک حریف می تواند یک پیشگویی رمزگشایی را برای رمزگشایی تعداد چندجمله ای متون رمزی درخواست نماید (به استثنای متن رمزی چالش c)، حریف می تواند هر متن رمزی داده شده c را با روش زیر رمزگشایی نماید. اول حریف پیشگویی برای رمزگشایی c′ را درخواست می کند، سپس پیشگویی $m' = m \oplus \delta m$ را درخواست می کند. لذا، او می تواند متن مهنادار هدف c را با $m = m' \oplus \delta m$ بازیابی کند.

4 تبدیلات برای McEliece PKC

همانطور که در بخش 3 ذکر شد، بدون هر پیشگویی رمزگشایی و هر دانش جزئی در مورد متن مهنادار متناظر برای متن رمزی چالش، هیچ الگوریتم چندجمله ای-زمانی برای تبدیل McEliece PKC شناخته شده نیست (که پارامترهای آن به دقت انتخاب می شوند). تحت این فرض که این مسئله تبدیل سخت است، این مسئله می تواند به مسئله ای سخت برای شکستن قابلیت تشخیص رمزگذاری در مقابل حملات بحرانی تبدیل شود (یا به طور کلی تر در مقابل حملات متن رمزی انتخاب شده تطبیقی) با معرفی تبدیلات مناسب در کد پیشگویی تصادفی. در این بخش، ما بررسی می کنیم که تبدیلات برای McEliece PKC مناسب هستند و اینکه نیستند.

4.1 دستورات

ما از دستورات زیر در این مقاله استفاده می کنیم:

C(n,t): تعداد ترکیبات با اتخاذ t از n عنصر

Prep(m): پیش پردازش برای یک پیام m مانند فشردگی داده ها، مسیر داده ها و غیره. معکوس آن به صورت $Prep^{-1}()$ نشان داده می شود.

Hash(x): تابع هش یک راهه برای رشته دودویی با طول دلخواه x برای یک رشته دودویی با طول ثابت. زمانی که حوزه خزوجی Zn که در آن N=C(n,t). ما از Hashz(x) به جای Hash(x) استفاده می کنیم.

Conv(z): تابع Bijective که یک عدد صحیح $\bar{z} \in Z_N$ را تبدیل می کند که در آن N=C(n,t) به بردار خطای متناظر z. معکوس آن به صورت $Conv^{-1}()$ نشان داده می شود.

Gen(x): تولیدکننده دنباله های شبه تصادفی امن رمزنگاری با طول دلخواه از بذر طول ثابت x.

Len(x): طول بیت x.

Msbx1(x2): بیت های x1 چپ x2.

Lsbx1(x2): بیت های x1 راست x2.

Const: ثابت از پیش تعیین شده استفاده شده در کل

Rand: منبع تصادفی که دنباله تصادفی صحیح (یا شبه تصادفی قابل تشخیص محاسباتی) را تولید می کند.

$\mathcal{E}^{McEliece}(x, z)$: رمزگذاری x با استفاده از McEliece PKC با بردار خطای z.

$\mathcal{D}^{McEliece}(x)$: رمزگشایی x با استفاده از McEliece PKC اصلی

4.2 تبدیلات نامناسب برای McEliece PKC

تبدیل OAEP. در [2] Bellar و Rogaway یک تبدیل عام به نام OAEP را پیشنهاد نمودند (پد رمزگشایی نامتقارن بهینه) که OWTP (جایگشت Trapdoor تک راهه) مانند اولیه RSA را به PKC تبدیل می کند که در مقابل حملات متن رمزی انتخاب شده تطبیق غیرقابل تشخیص است (CCA2). McEliece PKC با این تبدیل OAEP در شکل 1 نشان داده شده است. متاسفانه، این تبدیل به طور صحیح کار نمی کند زیرا حمله واکنش هنوز

قابل کاربرد است. این بدین معنی نیست که تبدیل OAEP دارای خطا است، اما McEliece اولیه یک جایگشت نیست.

تبدیل ساده Fujisaki-Okamoto. در [8]، Fujisaki and Okamoto یک تبدیل ساده و عام را از PKC پیشنهاد نمودند که در مقابل CPA (حملات متن مهنادار انتخاب شده) در یک PKC قابل تشخیص نیست که در مقابل CCA2 قابل تشخیص نیست. McEliece PKC با این تبدیل در شکل 2 نشان داده شده است. متاسفانه، این تبدیل به درستی کار نمی کند زیرا حمله متن مهنادار جزئی شناخته شده به درستی کار می کند مگر اینکه Len(r) نزدیک به k باشد.

این بدین معنی نیست که تبدیل ساده Fujisaki-Okamoto دارای خطا است، اما McEliece PKC حتی در مقابل CPA قابل تشخیص است. هر حریف مجهول (که از پیشگوییی رمزگشایی استفاده نمی کند) می تواند حدی بزند که کدام پیام m0 و m1 متن مهنادار متناظر متن رمزی معین c برای McEliece PKC اصلی با دیدن اینکه آیا وزن $m_b G' \oplus \bar{c}$ t است یا خیر که در آن $b \in \{0, 1\}$.

Encryption of m:

$$
\begin{aligned}
r, \bar{z} &:= Rand \\
\bar{m} &:= Prep(m) \\
y_1 &:= (\bar{m} || Const) \oplus Gen(r) \\
y_2 &:= r \oplus Hash(y_1) \\
z &:= Conv(\bar{z}) \\
c &:= \mathcal{E}^{McEliece}((y_1 || y_2), z)
\end{aligned}
$$

return c

شکل 1. تبدیل OAEP + McEliece PKC

Encryption of m:

$$
\begin{aligned}
r &:= Rand \\
\bar{m} &:= Prep(m) \\
z &:= Conv(Hash_z(\bar{m}||r)) \\
c &:= \mathcal{E}^{McEliece}((\bar{m}||r), z) \\
\text{return} \quad & c
\end{aligned}
$$

شکل 2. تبدیل ساده Fujisaki-Okamoto + McEliece PKC

Encryption of m:

$$
\begin{aligned}
r, r' &:= Rand \\
\bar{m} &:= Prep(m) \\
z &:= Conv(Hash_z(\bar{m}||r)) \\
y_1 &:= \mathcal{E}^{McEliece}(r', z) \\
y_2 &:= Gen(r') \oplus (\bar{m}||r) \\
c &:= y_1||y_2 \\
\text{return} \quad & c
\end{aligned}
$$

شکل 3. تبدیل عام Pointcheval

Encryption of m:

$$
\begin{aligned}
r &:= Rand \\
\bar{m} &:= Prep(m) \\
z &:= Conv(Hash_z(\bar{m}||r)) \\
y_1 &:= \mathcal{E}^{McEliece}(r, z) \\
y_2 &:= Gen(r) \oplus \bar{m} \\
c &:= y_1||y_2 \\
\text{return} \quad & c
\end{aligned}
$$

شکل 4. تبدیل عام Fujisaki-Okamoto

4.3 تبدیلات عام قابل کاربرد برای McEliece PKC

تبدیل عام Pointcheval. در [24]، Pointcheval یک تبدیل عام را از PTOWF (تابع تک راه دریچه جزئی) برای یک PKC پیشنهاد نمود که در مقابل CCA2 قابل تشخیص است.

تعریف f(x,y) برای PTOWF به صورت زیر است:

- حریف زمانی-چندجمله ای و برای هر z=f(x,y) معین، به طور محاسباتی بازگشت به پیش تصویر جزئی x غیرعملی است
- با برخی اطلاعات رمزی زیادی، بازگشت به x آسان است.

نه تنها اولیه های ElGamal[7], Okamoto-Uchiyama[22], Naccache-Stern[20] and Paillier[23] بلکه اولیه McEliece می تواند در PTOWF رده بندی شود. بنابراین تبدیل عام Pointcheval نیز برای McEliece PKC با اثباتی یکسان در [24] قابل کاربرد است. McEliece PKC با این تبدیل در شکل 3 نشان داده شده است.

تبدیل عام Fujisaki-Okamoto. در [9]، Fujisaki-Okamoto یک تبدیل عام را از OWE (رمزگذاری تک راهه) پیشنهاد نمودند که شامل OWTP و PTOWF در یک PKC با غیرقابل تشخیص بودن در مقابل ACC2 می شود.

Encryption of m:	**Decryption of c:**
$r := Rand$	$y_1 := \mathcal{D}^{McEliece}(Msb_n(c))$
$\bar{m} := Prep(m)$	$z := Msb_n(c) \oplus y_1 G'$
$\bar{z} := Hash_z(r\|\|\bar{m})$	$\bar{z} := Conv^{-1}(z)$
$(y_1\|\|y_2) := Gen(\bar{z}) \oplus (r\|\|\bar{m})$	$(r\|\|\bar{m}) := Gen(\bar{z}) \oplus (y_1\|\|y_2)$
$z := Conv(\bar{z})$	If $\bar{z}=Hash_z(r\|\|\bar{m})$
$c := \mathcal{E}^{McEliece}(y_1, z)\|\|y_2$	return $Prep^{-1}(\bar{m})$
return c	Otherwise reject c

شکل 5. تبدیل $\alpha : Len(y_1) = k \text{ and } Len(y_2) = Len(r||\bar{m}) - k.$ اگر $Len(r||\bar{m}) = k,$ را y2 حذف کند.

بدون نیاز به گفتن، اولیه McEliece می تواند در OWE رده بندی شود و بنابراین این تبدیل عام برای McEliece PKC با همان اثبات در [9] قابل کاربرد است. McEliece PKC با این تبدیل در شکل 4 نشان داده شده است.

4.4 تبدیلات خاص ما

در حالیکه می تواند McEliece PKC های امن معنادار را با به کارگیری ساده تبدیلات عام بالا طراحی نمود، آنها لزوماً برای McEliece PKC مناسب نیستند. چون اندازه بلوک McEliece PKC بزرگتر از PKCهای شناخته شده است، مانند RSA، سیستم های رمز منحنی بیضوی و غیره، افزونگی داده ها (که با تفاوت بین طول بیت متن مهنادار و متن رمزی متناظر آن تعریف می شود) بزرگ می شود. برای مثال، برای (n,k)=(4096,2560)، تبدیلات عام نیاز به 4096 بیت یا بیشتر برای داده های سرریز دارد. از طرف دیگر، تبدیلات توصیف شده ما در شکل 7~5 نیاز به داده های سرریز کمتر از داده های عام دارد. برای مثال، برای همان تنظیمات و Len(r)=160 و Len(Const)=160، تبدیل ما نیاز به تنها 1024 بیت دارد. (این می تواند هنوز بزرگ باشد اما از آن جالب تر این مقدار کمتر از McEliece PKC اولیه است). نتایج مقایسه در جدول 1 خلاصه شده است.

نقطه تبدیل اینست که نه تنها متن مهنادار بلکه بردار خطا از بخش y1 (یا $(y_2||y_1)$) گرفته می شود این کار سرزیر داده ها را حتی نسبت به McEliece PKC کاهش می دهد زمانی که $Len(r) + Len(Const) < |\log_2 C(n,t)|.$ مطالعه برای کاهش داده های سرریز (و به طور همزمان برای بهبود امنیت در مقابل حملات مرتبط با پیام) در [27] انجام شده است. در حالیکه تبدیلات او ارائه دهنده امنیت قابل اثبات در مقابل CCA2 نیست (زیرا حملات متن مهنادار جزئی شناخته شده یا حملات واکنش حداقل قابل کاربرد هستند)، روش او برای کاهش داده های سرریز باشد درک شود.

غیرقابل تشخیص بودن تبدیلات ما. به طور ذاتی مشخص است که تبدیلات ما در مقابل تمام حملات در بخش 3.2 مقاومت می کند زیرا برای

Encryption of m:	**Decryption of c:**
$r := Rand$	$y_4 := Msb_{Len(c)-n}(c)$
$\bar{m} := Prep(m)$	$y_3 := \mathcal{D}^{McEliece}(Lsb_n(c))$
$y_1 := Gen(r) \oplus \bar{m}$	$z := Lsb_n(c) \oplus y_3 G'$
$y_2 := r \oplus Hash(y_1)$	$(y_2 \| y_1) := (y_4 \| y_3)$
$(y_4 \| y_3) := (y_2 \| y_1)$	$r := y_2 \oplus Hash(y_1)$
$z := Conv(Hash_z(r))$	$\bar{m} := Gen(r) \oplus y_1$
$c := y_4 \| \mathcal{E}^{McEliece}(y_3, z)$	If $Conv^{-1}(z) = Hash_z(r)$
return c	return $Prep^{-1}(\bar{m})$
	Otherwise reject c

شکل 6. تبدیل $\beta : Len(y_3) = k \text{ and } Len(y_4) = Len(r\|\bar{m}) - k$ اگر $Len(r\|\bar{m}) = k,$ y4 را حذف کند.

Encryption of m:	**Decryption of c:**
$r := Rand$	$y_5 := Msb_{Len(c)-n}(c)$
$\bar{m} := Prep(m)$	$y_3 := \mathcal{D}^{McEliece}(Lsb_n(c))$
$y_1 := Gen(r) \oplus (\bar{m} \| Const)$	$z := y_3 G' \oplus Lsb_n(c)$
$y_2 := r \oplus Hash(y_1)$	$\bar{z} := Conv^{-1}(z)$
$(y_5 \| y_4 \| y_3) := (y_2 \| y_1)$	$y_4 := Lsb_{\lfloor \log_2 C(n,t) \rfloor}(\bar{z})$
$z := Conv(y_4)$	$(y_2 \| y_1) := (y_5 \| y_4 \| y_3)$
$c := y_5 \| \mathcal{E}^{McEliece}(y_3, z)$	$r := y_2 \oplus Hash(y_1)$
return c	$(\bar{m} \| Const') := y_1 \oplus Gen(r)$
	If $Const' = Const$
	return $Prep^{-1}(\bar{m})$
	Otherwise reject c

شکل 7. تبدیل $\gamma : Len(y_3) = k,\ Len(y_4) = \lfloor \log_2 C(n,t) \rfloor,\ Len(y_5) = Len(\bar{m}) +$

$$Len(Const) + Len(r) - Len(y_4) - k$$

اگر

$$Len(\bar{m}) + Len(Const) + Len(r) = Len(y_4) + k,$$

y5 را حذف کند.

حریفان، سود استعمال از پیشگویی های رمزگشایی سخت است به علت مشکل تولید متن رمزی مناسب بدون دانستن متن مهنادار آن و حدس زدن ورودی برای McEliece PKC اصلی آن نیز در تبدیلات ما به همچنین حتی اگر آنها متن مهنادار را برای تبدیلات ما بدانند.

به طور رسمی تر، قضیه زیر برای تبدیلات ما در مدل پیشگویی تصادفی درست است (که در آن Gen,Hash و Hashz ایده آل فرض شوند)

قضیه 1. برای شکستن غیرقابل تشخیص بودن رمزگریذا تبدیلات خاص ما در سناریوی متن رمزی-انتخاب شده-تطبیقی، چندجمله ای معادل برای رمزگشایی کل متن مهنادار برای متن رمزی معین دلخواه McEliece PKC اصلی بدون هر کمک پیشگویی ها رمزگشایی و هر دانش در مورد متن مهنادار هدف وجود دارد.

Conversion Scheme	Conversion Type	Complexity*2 / Data Redundancy*1 = Ciphertext Size - Plaintext Size (n,k) t	$\geq 2^{56.3}$ $(1024, 644)$ 38	$\geq 2^{101.9}$ $(2048, 1289)$ 69	$\geq 2^{186.2}$ $(4096, 2560)$ 128
Pointcheval's [24]	Generic	$n + Len(r)$	1184	2208	4256
Fujisaki -Okamoto's [9]	Generic	n	1024	2048	4096
Our proposal α and β	Specific	$n - k + Len(r)$	540	919	1696
Our proposal γ	Specific	$n - k + Len(r)$ $+Len(Const)$ $-\lfloor \log_2 C(n,t) \rfloor$	470	648	1040
Original McEliece	None	n-k	380	759	1536

جدول 1. مقایسه بین افزونگی داده ها و تبدیلات

1 نتایج عددی تحت این تنظیم به دست می آیند که Len(r)=160 و Len(Const)=160

2 مرز پایینی مجانبی تعداد مورد انتظار تکرارها برای تبدیل متن رمزی دلخواه McEliece PKC اصلی با استفاده از حمله یافتن-کلمه کد-وزن-پایین. پیچیدگی دقیق در [4] تخمین زده شده است.

توجه کنید که همانطور که در بخش 3 ذکر شد، هنوز رمزگشایی کل متن مهنادار برای متن رمزی معین دلخواه McEliece PKC با پارامترهای مناسب (بدون هر کمکی به پیشگویی های رمزگشایی و هر دانش در مورد متن مهنادار هدف) غیرعملی است.

این قضیه می تواند در مدل پیشگویی تصادفی با نشان داده اینکه چگونه یک الگوریتم ساخته می شود اثبات شود که یک متن رمزی دلخواه McEliece PKC اصلی را با استفاده از یک الگوریتم رمزگشایی می کند که متن رمزی نسخه های تبدیل شده را در سناریوی متن رمزی-انتخاب شده-تطبیقی تمییز می کند (مشخص است که یک الگوریتم که می تواندMcEliece PKC اصلی را رمزگشایی کند، می تواند یک متن رمزی را برای نسخه های تبدیل شده ما تمییز کند). جزئیات در پیوست A توصیف شده است.

5 نتیجه گیری

ما به دقت حملات شناخته شده جاری را برای McEliece PKC بازنگری نمودیم و سپس تایید نمودیم که بدون هر پیشگویی رمزگشایی و هر دانش جزئی رد مورد متن مهنادار متناظر متن رمزی چالش، بدون الگوریتم زمانی-چندجمله ای برای تبدیل McEliece PKC شناخته شده است که پارامترهای آن به دقت انتخاب می شوند. تحت این فرض که این مسئله تبدیل سخت است، ما در مد پیشگویی تصادفی بررسی نمودیم که چگونه تبدیل این مسئله سخت به مسئله سخت شکستن غیرقابل تشخیص بودن رمزگذاری با CCA2 صورت می گیرد. در حالیکه برخی از تبدیلات عام برای McEliece PKC قابل کاربرد است، آنها دارای عیبی در افزونگی داده ها هستند. میزان زیادی از داده های افزونه برای تبدیلات عام نیاز می شود زیرا اندازه بلوک McEliece PKC نسبتاً بزرگ است. تبدیلات خاص ما می تواند کاهش داده های افزونه را به 1/3~1/4 در مقایسه با تبدیلات عام برای پارامترهای عملی حاصل نماید. این بدین معنی است که حدود 3K بیت می تواند برای n=4096 با ارائه نمودن امنیت معنایی در مقابل CCA2 ذخیره شود.

تشکرات

نویسندگان خواهان تشکر از and Yuliang Zheng Hung-Min Sun, Pierre Loidreau, Kwangjo Kim برای بررسی ها و اظهار نظرات مفید آنها هستند.

اثبات قضیه 1

A.1 غیرقابل تشخیص بودن رمزگذاری

دستور امنیتی به نام غیرقابل تشخیص بودن رمزگذاری را به خاطر آورید [11]. در این دستور، یک حریف دو متن مهنادار m0 و m1 را با طول یکسان در مرحله یافتن انتخاب می کند و سپس در مرحله حدس، c A داده شده است که رمزگذاری mb است که در آن b 0 یا 1 با احتمال ½ است. سپس، A سعی در حدس زدن b دارد. مزیت A با 2Pr(Win)-1 تعریف می شود که در آن Pr(Win) نشاندهنده احتمال مورد انتظار A با حدس زدن b به طور صحیح است. اگر A دارای پیشگویی رمزگشایی D باشد (که هر متن رمزی دیگر را نسبت به متن رمزی c رمزگشایی می کند)، مشخص می شود که این آزمایش در سناریویی متن رمزی-انتخاب شده تطبیقی است. در غیراینصورت، اگر A آن را نداشته باشد، مشخص می شود این آزمایش در سناریوی متن مهنادار-انتخاب شده-تطبیقی است.

A.2 پیشگویی تصادفی

یک پیشگویی تصادفی، یک هش ایده آل یا تولیدکننده ایده آل است که به طور صحیح تعداد تصادفی توزیع شده به طور یکنواخت در ناحیه خروجی برای پرس و جوی جدید باز می گرداند، اما همان مقدار را برای همان پرس و جو باز می گرداند. در چنین پیشگویی های تصادفی، لم زیر صحیح است.

لم 1 فرض کنید که f یک پیشگویی تصادفی است. بنابراین رسیدن به اطلاعات مهم در مورد f(x) بدون درخواست x برای پیشگویی غیرممکن است حتی اگر کسی تمام خروجی های دیگر را برای f به جز مورد متناظر با x بشناسد.

مشخص است که لم 1 صحیح است زیرا مقدار خروجی f به طور صحیح تصادفی است.

A.3 امنیت متن رمزی-انتخاب شده-تطبیقی

References

1. C. M. Adams and H. Meijer. "Security-Related Comments Regarding McEliece's Public-Key Cryptosystem". In *Proc. of CRYPTO '87, LNCS 293*, pages 224–228. Springer–Verlag, 1988.
2. M. Bellare and P. Rogaway. "Optimal Asymmetric Encryption". In *Proc. of EUROCRYPT '94, LNCS 950*, pages 92–111, 1995.
3. T. Berson. "Failure of the McEliece Public-Key Cryptosystem Under Message-Resend and Related-Message Attack". In *Proc. of CRYPTO '97, LNCS 1294*, pages 213–220. Springer–Verlag, 1997.
4. A. Canteaut and N. Sendrier. "Cryptoanalysis of the Original McEliece Cryptosystem". In *Proc. of ASIACRYPT '98*, pages 187–199, 1998.
5. W. Diffie and M. Hellman. "New directions in cryptography". *IEEE Trans. IT*, 22(6):644–654, 1976.
6. D. Dolve, C. Dwork, and M. Naor. "Non-Malleable Cryptography". In *Proc. of the 23rd STOC*. ACM Press, 1991.
7. T. ElGamal. "A public-key cryptosystem and a signature scheme bsed on discrete logarithms". In *Proc. of CRYPTO '84*, pages 10–18, 1985.
8. E. Fujisaki and T. Okamoto. "How to Enhance the Security of Public-Key Encryption at Minimum Cost". In *Proc. of PKC'99, LNCS 1560*, pages 53–68, 1999.
9. E. Fujisaki and T. Okamoto. "Secure Integration of Asymmetric and Symmetric Encryption Schemes". In *Proc. of CRYPTO '99, LNCS 1666*, pages 535–554, 1999.
10. J. K. Gibson. "Equivalent Goppa Codes and Trapdoors to McEliece's Public Key Cryptosystem". In *Proc. of EUROCRYPT '91, LNCS 547*, pages 517–521. Springer–Verlag, 1991.
11. S. Goldwasser and S. Micali. "Probabilistic encryption". *Journal of Computer and System Sciences*, pages 270–299, 1984.
12. C. Hall, I. Goldberg, and B. Schneier. "Reaction Attacks Against Several Public-Key Cryptosystems". In *Proc. of the 2nd International Conference on Information and Communications Security (ICICS'99), LNCS 1726*, pages 2–12, 1999.
13. K. Kobara and H. Imai. "Countermeasure against Reaction Attacks (in Japanese)". In *The 2000 Symposium on Cryptography and Information Security : A12*, January 2000.
14. V.I. Korzhik and A.I. Turkin. "Cryptanalysis of McEliece's Public-Key Cryptosystem". In *Proc. of EUROCRYPT '91, LNCS 547*, pages 68–70. Springer–Verlag, 1991.
15. P. J. Lee and E. F. Brickell. "An Observation on the Security of McEliece's Public-Key Cryptosystem". In *Proc. of EUROCRYPT '88, LNCS 330*, pages 275–280. Springer–Verlag, 1988.
16. P. Loidreau. "Strengthening McEliece Cryptosystem". In *Proc. of ASIACRYPT 2000*. Springer–Verlag, 2000.
17. P. Loidreau and N. Sendrier. "Some weak keys in McEliece public-key cryptosystem". In *Proc. of IEEE International Symposium on Information Theory, ISIT '98*, page 382, 1998.
18. R. J. McEliece. "A Public-Key Cryptosystem Based on Algebraic Coding Theory". In *Deep Space Network Progress Report*, 1978.
19. A. J. Menezes, P. C. Oorschot, and S. A. Vanstone. "McEliece public-key encryption". In *"Handbook of Applied Cryptography"*, page 299. CRC Press, 1997.
20. D. Naccache and J. Stern. "A New Cryptosystem based on Higher Residues". In *Proc. of the 5th CCS*, pages 59–66. ACM Press, 1998.
21. T. Okamoto, K. Tanaka, and S. Uchiyama. "Quantum Public-Key Cryptosystems". In *Proc. of CRYPTO 2000, LNCS 1880*, pages 147–165. Springer–Verlag, 2000.
22. T. Okamoto and S. Uchiyama. "A New Public Key Cryptosystem as Secure as Factoring". In *Proc. of EUROCRYPT '98, LNCS 1403*, pages 129–146, 1999.
23. P. Paillier. "Public-Key Cryptosystems Based on Discrete Logarithms Residues". In *Proc. of EUROCRYPT '99, LNCS 1592*, pages 223–238. Springer–Verlag, 1999.
24. D. Pointcheval. "Chosen-Ciphertext Security for Any One-Way Cryptosystem". In *Proc. of PKC 2000, LNCS 1751*, pages 129–146. Springer–Verlag, 2000.
25. P.W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal on Computing*, 26:1484–1509, 1997.
26. J. Stern. "A method for finding codewords of small weight". In *Proc. of Coding Theory and Applications , LNCS 388*, pages 106–113. Springer–Verlag, 1989.
27. H. M. Sun. "Improving the Security of the McEliece Public-Key Cryptosystem". In *Proc. of ASIACRYPT '98*, pages 200–213, 1998.
28. H. M. Sun. "Further Cryptanalysis of the McEliece Public-Key Cryptosystem". *IEEE Trans. on communication letters*, 4:18–19, 2000.
29. A. Vardy. "The Intractability of Computing the Minimum Distance of a Code". *IEEE Trans. on IT*, 43:1757–1766, 1997.