ỨNG DỤNG MẬT MÃ LƯỢNG TỬ TRONG AN TOÀN THÔNG TIN

TS. Ngô Tứ Thành, TS. Lê Minh Thanh

Các báo, tạp chí trong và ngoài nước đã từng liên tục đưa các tin như: "Tập đoàn viễn thông khổng lồ của Nhật Bản Mitsubishi Electric mới truyền được một bản mật mã lượng tử đi xa 87 km bằng cáp quang" - "Công ty iD Quantique (Thuỵ Sỹ) đã tung ra thị trường các thiết bị bảo vệ dữ liệu nhạy cảm bằng loại mật mã lượng tử", - "Một ngân hàng ảo vừa triển khai loại hình chuyển tiền điện tử bằng cách sử dụng mật mã lượng tử v.v... Vậy "mật mã lượng tử" là gì? Vì sao lại được các phương tiện thông tin quan tâm như vậy? Bài viết sẽ giải đáp các câu hỏi trên.

1/ LÝ DO PHÁT TRIỂN MẬT MÃ LƯỢNG TỬ

1.1 Mối đe dọa "máy tính lượng tử" đối với an toàn thông tin

Theo ý kiến của các chuyên gia, khi máy tính lượng tử ra đời, khả năng tính toán của nó mạnh tới mức sẽ giải mã được tất cả các hệ thống mật mã hiện hành. Một máy tính lượng tử chỉ với 30 qubit đã đạt tốc độ tính toán 10 teraops (mười tỷ tỷ phép toán trên một giây). Trong khi đó máy siêu tính nhanh nhất ngày nay, với hàng tỷ bit, chỉ là 2 teraops. Để có thể giải mã những hệ thống mật mã phức tạp nhất, các máy siêu tính ngày nay phải chạy trong hàng triệu năm. Trong khi đó, một máy tính lượng tử hoàn chỉnh, với nhiều qubit, giải mã đó chỉ trong vòng vài phần giây. Lúc đó không có gì trên Internet là an toàn... với máy 30 qubit, các phương pháp mật mã ngày nay là vô nghĩa...

Tuy nhiên việc ra đời máy tính lượng tử chưa phải là lý do chính đe dọa trực tiếp đến an toàn thông tin hiện nay. Vì việc xây dựng máy tính lượng tử là rất phức tạp và chưa khả thi trong tương lai gần. Người phát ngôn của Hãng NET Nhật Bản năm 2003 tuyên bố "Máy tính lượng tử hiện thực sẽ chỉ xuất hiện đại trà sau năm 2020".

1.2 Không thể có bảo mật tuyệt đối theo lý thuyết thông tin cổ điển

Theo lý thuyết thông tin của Shannon, nếu gọi X là một biến ngẫu nhiên có các giá trị $\{x_1,x_2,....x_n\}$ với các xác suất lần lượt $\{p_1,p_2,....p_n\}$ thì entropy của nó được định nghĩa như sau:

$$H(X) = -\sum_{i=1}^{n} p_i \cdot \log(p_i)$$

H(X/Y) là Entropy có điều kiện đặc trưng cho độ bất định về nguồn tin X sau khi nhận được các tin Y:

$$H(X/Y) = -\sum_{x\in X, y\in Y} p(x,y) \cdot \log(p(x/y))$$

Một hệ mật mã được đặc trưng bởi 3 biến
- M: tập hợp các thông điệp rõ (plaintexts)
- K: tập hợp các khóa
- C: tập hợp các thông điệp được mật mã hóa (ciphertexts)

Một hệ được gọi là an toàn tuyệt đối nếu sau khi nhận được thông điệp mật mã hóa, người nhận không có được thêm thông tin gì về thông điệp rõ tương ứng. Nói một cách khác, xác suất thông điệp rõ lấy giá trị m (thuộc tập hợp M) sau khi đã biết thông điệp được mật mã hóa của nó vẫn bằng xác suất thông điệp lấy giá trị m trước đó:

Nghĩa là $\forall m \in M$ và $\forall c \in C$ thì p(m/c)=p(m). Do đó: H(M/C) =H(M)

Theo lý thuyết của Shannon: nếu một hệ mật mã (M, K, C) là an toàn tuyệt đối thì

$$|K| \geq |C| \geq |M|$$

có nghĩa là một hệ mật mã an toàn hoàn hảo cần một số lượng khóa ít nhất nhiều như số lượng thông điệp. Trong trường hợp tối ưu, $|K| = |C| = |M|$, chúng ta có giao thức

trao đổi thông tin an toàn vô điều kiện của Vernam như sau :

Để trao đổi mỗi thông điệp m, Alice (người gửi) và Bob (người nhận) sử dụng một dãy bit ngẫu nhiên - k - có cùng độ dài với thông điệp làm khóa bí mật. Alice tổ hợp thông điệp với khóa để tạo ra thông điệp mật mã $c_i = m_i \oplus k_i$, *ở đây là phép cộng modulo 2. Bob giải mã thông điệp bằng cùng một thuật toán, tức là* $m_i = c_i \oplus k_i$. *Mỗi khóa k chỉ được sử dụng 1 lần.*

Nếu một khóa được sử dụng nhiều lần thì người ta có thể chứng minh về mặt toán học và thống kê được rằng đối phương có thể tìm ra được khóa sau khi đã biết được một số lượng đủ thông điệp được mã bằng khóa này.

Như vậy, để có được sự an toàn tuyệt đối, mỗi khóa chỉ được sử dụng 1 lần! Bài toán phân phối khóa trở nên phức tạp. Giải pháp sử dụng khóa công khai để phân phối khóa bí mật rõ ràng không tối ưu. Tóm lại trong hệ mật mã cổ điển thông tin muốn được bảo mật an toàn tuyệt đối nhất vẫn là dùng... người (giao liên), một giải pháp tốn kém, bất tiện và không phải lúc nào cũng thực hiện được.

Trong khi đó Mật mã lượng tử, bằng việc gửi và nhận thông tin lượng tử lại tỏ ra dễ dàng hơn và đã thực hiện thành công trên các hạt ánh sáng (photon). Mật mã lượng tử đã mở ra triển vọng đảm bảo giải quyết vấn đề mà mật mã cổ điển không giải quyết được.

2. MẬT MÃ LƯỢNG TỬ (QUANTUM CRYPTOGRAPHY - QC)

2.1 Cơ sở khoa học hình thành mật mã lượng tử

Mật mã lượng tử là bộ phận quan trọng cấu thành thông tin lượng tử. Thông tin lượng tử là khoa học sử dụng các đặc tính và nguyên lý của cơ học lượng tử để xử lý và truyền thông tin. Nếu như mật mã cổ điển khai thác độ khó các thuật toán, thuộc lĩnh vực ngành toán tin, thì mật mã lượng tử khai thác các tính chất của cơ học lượng tử. Những nguyên lý cơ bản của cơ học lượng tử được sử dụng trong thông tin và mật mã lượng tử gồm:

- Nguyên lý bất định của Heisenberg: người ta không bao giờ có thể xác định chính xác cả vị trí lẫn vận tốc của một hạt vào cùng một lúc. Nếu ta biết một đại lượng càng chính xác thì ta biết đại lượng kia càng kém chính xác.

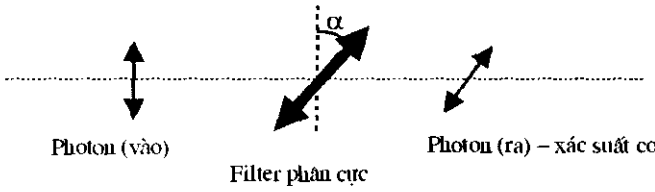
- Không thể sao chép (no-clonning): dựa trên nguyên lý bất định, vì không thể biết chắc chắn trạng thái một hệ thống lượng tử nên không thể sao chép hoàn hảo một hệ thống lượng tử bất kỳ.

- Tính chất vướng víu (entanglement): một hệ thống lượng tử có tương quan (correlated) với một hay nhiều hệ thống lượng tử khác. Mỗi phân hệ sinh ngẫu nhiên ra trạng thái của mình và không một phân hệ nào có trạng thái cố định.

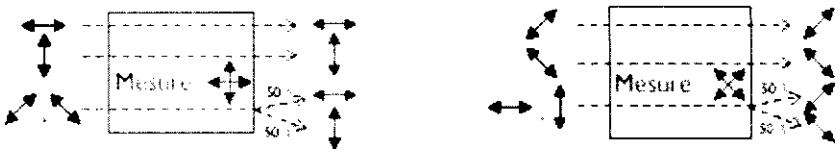
Vật lý đã chứng minh ánh sáng vừa có tính chất hạt, vừa có tính chất sóng. Một photon có thể xem như một điện trường tí hon dao động. Hướng dao động của điện trường là sự phân cực (polarization) của photon. Khi cho photon đi qua một bộ lọc phân cực (polarised filter) thì các photon, hoặc là bị bộ lọc hấp thụ, hoặc được truyền đi nhưng với sự phân cực của bộ lọc! Và xác suất của photon được truyền qua bộ lọc là $\cos^2(\alpha)$, trong đó α là góc phân cực của photon so với góc phân cực của bộ lọc (Hình 1).

Trên hình 1 dễ ràng thấy rằng nếu phân cực photon song song với bộ lọc thì nó chắc chắn sẽ được truyền qua ($\cos^2(0^o) = 1$). Nếu vuông góc thì nó sẽ bị bộ lọc hấp thụ hoàn toàn ($\cos^2(90^o) = 0$). Việc photon được truyền qua bộ lọc hay bị hấp thụ sẽ hoàn toàn ngẫu nhiên nếu $\alpha = 45^o$ hoặc 135^o ($\cos^2(\alpha) = 1/2$). Photon sau khi ra khỏi bộ lọc bị mất hoàn toàn thông tin về góc phân cực trước đó của nó, hay nói một cách khác, người ta không thể sao lại trạng thái phân cực của một photon để thực hiện nhiều phép đo sự phân cực của nó với các bộ lọc phân cực khác nhau.

Như vậy, khi cho một chùm photon đi qua một bộ lọc phân cực, các photon thu được sẽ có cùng mặt phẳng phân cực của bộ lọc. Đây chính là nguyên tắc lập mã cho



Hình 1: Sự phân cực của photon khi qua bộ lọc phân cực



Hình 2: Đo phân cực photon bằng các hệ phân cực cơ sở thẳng và chéo

photon. Bộ lọc phân cực cũng được dùng để xác định trạng thái phân cực của photon. Ví dụ nếu nguồn photon chỉ gồm những photon có các góc phân cực 0° và 90° thì dùng một bộ lọc 0°, người ta có thể xác định được chính xác những photon 0° (qua) và 90° (không qua). Thao tác này gọi là phép đo phân cực của photon. Một cặp bộ lọc phân cực trực giao để lập mã hoặc đo photon được gọi là một phân cực cơ sở (base). Người ta có thể sử dụng một phân cực cơ sở để biểu diễn các giá trị 0 và 1 bằng các photon.

Hai phân cực cơ sở trực giao được sử dụng để mã hóa/đo các bit 0 và 1 cho các photon là: thẳng (0°/90°) - ký hiệu ⊕ và chéo (45°/135°) - ký hiệu ⊗. Trong phân cực cơ sở thẳng, các photon có góc phân cực 0° được tương ứng với bit 1, photon có phân cực 90° với bít 0. Tương tự trong hệ phân cực cơ sở chéo, các bít này tương ứng với các photon có góc phân cực lần lượt là 45° và 135°. Theo hình 2 dễ thấy rằng nếu các photon không cùng phân cực cơ sở với bộ đo, chúng ta sẽ thu được kết quả hoàn toàn ngẫu nhiên.

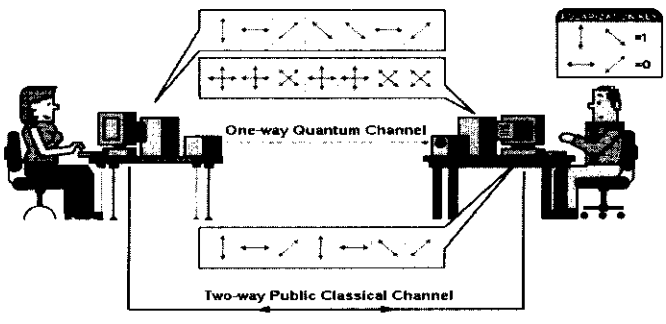
2.2 Giao thức phân phối khóa lượng tử (Quantum Key Distribution - QKD)

Vào đầu những năm 80, Bennett và Brassard đã tìm ra giao thức truyền khóa bí mật đầu tiên, công bố vào năm 1984, lấy tên là giao thức BB84. Điểm mấu chốt cho phép thực hiện BB84 cũng như tất cả các giao thức truyền khóa lượng tử được dựa trên tính chất bất định và không sao chép được của các trạng thái lượng tử: kẻ nghe trộm trên đường truyền (Eve) không thể đọc thông tin mà không làm thay đổi các trạng thái lượng tử, vì như vậy, sẽ để lại vết và bị phát hiện.

Mô hình trên hình 3 gồm: Alice (người gửi bên trái) có một chuỗi các phép đo (nhận giá trị hoặc thẳng hoặc chéo) và sinh một chuỗi ngẫu nhiên các photon phân cực theo phép đo. Bob (người nhận bên phải) sẽ dùng một chuỗi ngẫu nhiên các phép đo kiểm tra sự phân cực của các photon. Sau đó Bob thông báo chuỗi các phép đo của mình cho Alice, Alice thông báo các phép đo phù hợp, Bob giữ lại những kết quả trên các phép đo đó và chuyển đổi thành chuỗi {0,1}. Như vậy Alice và Bob đã có một chuỗi bit chung để làm khoá. Nếu sau khi truyền khóa xong, người dùng phát hiện có kẻ nghe trộm (Eva), họ có thể hủy bỏ kết quả và thực hiện truyền một khóa khác, không làm ảnh hưởng đến thông tin cần bảo mật của mình. Sau khi BB84 ra đời, nhiều giao thức khác cũng lần lượt được đề xuất, nổi bật là giao thức của Ekert đưa ra năm 1991 dựa trên các cặp vướng víu ("entangled"). Giao thức sử dụng các cặp "vướng víu" là tương đương với BB84, và hai giao thức này được tổng quát thành giao thức BBM92. Nhiều công trình nghiên cứu đã chứng minh: các giao thức truyền khóa lượng tử BBM92 đảm bảo sự an toàn tuyệt đối. Cho đến hiện nay chưa ai có thể xây dựng nên một hệ thống nghe trộm đặt trên đường truyền khóa lượng tử, và nếu có thường đòi hỏi chi phí khá lớn.

3. CÁC PHƯƠNG THỨC SỬ DỤNG MẬT MÃ LƯỢNG TỬ TRONG AN TOÀN THÔNG TIN

Mật mã lượng tử hiện chưa có ý định thay thế mật mã hiện nay, nó chỉ đóng góp một số mặt mạnh của tính chất lượng tử vào các hệ thống sẵn có, nghĩa là kết hợp với các hệ thống viễn thông hiện nay để nâng cao độ an toàn thông tin.



Hình 3. Mô hình Alice và Bob thực hiện BB84

3.1 Kết hợp giao thức QKD với truyền thông lượng tử (teleportation) xây dựng mạng truyền thông an toàn

Các nghiên cứu về "truyền thông lượng tử" hiện đã trở thành hiện thực ([1]) Tính an toàn của các giao thức QKD dựa trên tính chất không nhân đôi được của các trạng thái lượng tử. Do đó có thể tạo nên các "chặng" QKD chia sẻ các khóa giữa các nút trên đường truyền giữa 2 đầu cuối và dùng phép mã hóa Vernam để truyền một khóa cuối cùng giữa 2 đầu cuối. Sau đó sử dụng "truyền thông lượng tử" (teleportation) để tạo nên những trạm chuyển tiếp và các photon sẽ được "teleport" liên tiếp đến nút cuối.

3.2 Kết hợp giao thức QKD với mạng TCP/IP

Đặc tính "peer-to-peer" chỉ cho phép truyền khóa giữa 2 nút là một vấn đề nghiên cứu của các hệ thống QKD. Thông tin lượng tử không thể được sao chép hay broadcast trên mạng. Vậy nên các nghiên cứu xây dựng nên một mạng với topology cũng như các giao thức phụ trợ để có thể truyền thông tin an toàn trên toàn mạng là đề tài còn để ngỏ và cho ra nhiều định hướng khác nhau. Một ví dụ điển hình là dự án của DARPA cho xây dựng một mạng tích hợp các đường truyền QKD với hệ thống IPSec của mạng TCP/IP

3.3 Kết hợp hệ thống vệ tinh

Kết hợp hệ thống vệ tinh trong không trung có thể nới rộng khoảng cách địa lý, tăng khả năng truyền khoá lượng tử dẫn đến có thể truyền khoá trên phạm vi toàn cầu. Đây là phương thức nghiên cứu đầy triển vọng đang được các nhà khoa học trên thế giới quan tâm nghiên cứu.

4. TÌNH HÌNH VÀ KẾT QUẢ NGHIÊN CỨU VỀ MẬT MÃ LƯỢNG TỬ HIỆN NAY

4.1 Tình hình nghiên cứu mật mã lượng tử trên thế giới

Kể từ thử nghiệm thành công đầu tiên của 5 người Bennett, Bessette, Brassard, Salvail và Smolin trên một khoảng cách khiêm tốn 32 cm, các kết quả mới nhất đã có thể cho phép truyền khoá ở khoảng cách hàng trăm kilo mét nếu dùng sợi cáp quang và hàng vài chục kilô-mét trong không khí. Những khoảng cách này đã cho nhìn thấy tầm thực tiễn của các thiết bị truyền khoá lượng tử, lôi kéo sự tham gia của giới công nghiệp, ngân hàng và quân đội tham gia đầu tư. Đã có những thiết bị QKD được tung ra thị trường, mặc dù với giá khá đắt (http://www.idquantique.com/).

DARPA, cơ quan nghiên cứu của Bộ Quốc phòng Mỹ, cha đẻ của mạng DARPA - tiền thân của mạng Internet ngày nay, cũng đã xúc tiến tài trợ một chương trình do công ty BBN Technologies thầu nhằm xây dựng một mạng nhỏ sử dụng cơ chế truyền khoá an toàn mới mẻ này. Hiện nay mạng DARPA lượng tử này đã nối được cỡ chục nút mạng giữa các đối tác: trụ sở của công ty BBN Technologies, DARPA, các Đại học Havard, Boston. Cũng như DARPA cổ điển, mạng DARPA lượng tử mới này sẽ là tiền thân của một mạng lượng tử toàn cầu.

Độc lập và cạnh tranh với dự án của Mỹ, các nhà nghiên cứu và công nghiệp châu Âu cũng nhảy vào cuộc với dự án SECOQC (http://www.secoqc.net/), tìm kiếm một giải pháp mạng truyền thông an toàn cho nền kinh tế châu Âu chống lại sự đe doạ từ Mỹ. Đây là một dự án lớn, được chia làm 8 dự án con do các trung tâm nghiên cứu của châu Âu đảm nhiệm, trong đó trường Viễn thông Paris (ENST) tham gia vào dự án con / Kiến trúc mạng (Network Architecture). Mục đích của dự án con này là thiết kế và xây dựng một hạ tầng mạng mở cho phép tích hợp dễ dàng các đường truyền khoá lượng tử.

Công ty Magiq (Mỹ) và Công ty ID Quantique (Thuỵ Sĩ) đã tung ra thị trường các thiết bị bảo vệ dữ liệu nhạy cảm bằng loại mật mã lượng tử. Khi được kết nối với một mạng cáp quang, thiết bị QPN Security Gateway, trị giá 50.000-100.000 USD, của Magiq cho phép các công ty thành lập một mạng lưới ảo, có thể sử dụng mạng lưới này để gửi dữ liệu được mã hoá bằng các khoá lượng tử hoặc xác minh dữ liệu. Mã hoá lượng tử đã được thiết lập trong các phòng thí nghiệm nhiều năm qua song các kỹ sư của Magiq đã biến nó thành thiết bị thương mại.

Năm 2004 là năm mật mã lượng tử được sử dụng trong giao dịch thương mại lần đầu tiên. Ngày 21/4, Thị trưởng thành Viên đã chuyển tiền từ Tòa Thị chính đến Ngân hàng Cơ sở Tín dụng Áo (Austria Creditanstalt) qua cáp quang sử dụng khóa lượng tử được làm từ đơn quang tử (single photon) để đảm bảo chắc chắn là việc chuyển tiền hoàn toàn an toàn. Khóa lượng tử được phát ra ở ngân

hàng bằng cách sử dụng một tinh thể để chuyển quang tử từ một máy laser thành cặp quang tử "vướng víu" (entangled): một quang tử trong mỗi cặp ở lại ngân hàng, còn quang tử kia được gửi tới Tòa Thị chính. Bằng cách đo độ phân cực của quang tử, hai bên có thể tạo ra những chuỗi số 1 và 0 đồng nhất để có thể sử dụng như là một cái khóa.

4.2 Tình hình nghiên cứu mật mã lượng tử ở Việt Nam

Hiện nay ở Việt Nam: Công nghệ thông tin, Truyền thông và Vật lý chưa có tiếng nói chung. Công nghệ "Thông tin lượng tử" nói chung, mật mã lượng tử nói riêng vẫn còn là "giang sơn" và là đối tượng nghiên cứu của các nhà Vật lý lý thuyết. Còn những nhà khoa học, nhà quản lý về Công nghệ thông tin, truyền thông chưa có điều kiện nghiên cứu bản chất vật lý, bản chất bên trong, bước đột phá mới cũng như ảnh hưởng của "Thông tin lượng tử" trong tương lai. Do đó vấn đề nhận thức cũng như đầu tư nghiên cứu lĩnh vực này còn ở mức "khiêm tốn". Các kết quả nghiên cứu mới dừng lại ở các bài báo khoa học mang tính tổng quan, dịch thuật...

KẾT LUẬN

Thông tin lượng tử và mật mã lượng tử đã mở ra những triển vọng mới chưa từng có cho việc bảo mật thông tin trao đổi trên mạng. Tính an toàn vô điều kiện của các giao thức trao đổi khóa không phải do độ phức tạp thuật toán quyết định mà được đảm bảo bởi những luật tự nhiên của cơ học lượng tử. Nhiều dự án nghiên cứu đầy tham vọng nhằm vào việc xây dựng một mạng thông tin lượng tử trên qui mô toàn cầu đang được triển khai rầm rộ ở Mỹ và Tây Âu, với sự góp mặt của nhiều phòng thí nghiệm, Đại học và Trung tâm nghiên cứu uy tín trong nhiều lĩnh vực và nhiều quốc gia.

Còn rất nhiều vấn đề khó khăn chưa được giải quyết trong thông tin lượng tử nói chung và mật mã lượng tử nói riêng. Những nghiên cứu về thông tin lượng tử đòi hỏi kiến thức đa ngành nên cần có sự phối hợp của các chuyên gia trong nhiều lĩnh vực khác nhau: vật lý, toán học, công nghệ thông tin, mật mã học, lý thuyết thông tin và ngôn ngữ. Bài này đã tập trung vấn đề trao đổi khóa lượng tử trong mật mã lượng tử. Chúng tôi cho rằng đây là một hướng nghiên mới đầy triển vọng mà các nhà khoa học Việt Nam hoàn toàn có thể tham gia.

Tài liệu tham khảo

[1]. NGÔ TỨ THÀNH, LÊ MINH THANH, *Truyền thông lượng tử*, Tạp chí PC World tháng 4/2005

[2]. Beyond reality, New Scientist 14 March 1998

[3]. ANTON ZEILLINGER, *Experiment and the foundations of quantum physics*, Rev.Mod.Vol.71,No.2,Centenary 1999.

[4]. WOLFGANG TITTEL, GRÉGOIRE RIBORDY and NICOLAS GISIN, *informationAnton Zeillinger*, Quantum, Physics World March 1998.

[5]. DANIEL JONATHAN and MARTIN B.PLENO, *Entanglement-assited local manipulation of pure quantum states*, Blackett Laboratary, Imperial College Londo SW7 2BZ, United Kingdom

[6]. http://math.uwyo.edu/~moohous/quantum/

[7]. http://www.research.att.com/~shor/papers/ICM.pdf

[8]. http://www.idquantique.com/

[9]. http://www.secoqc.net/)

CHÂU ÂU: ĐỔ XÔ ĐĂNG KÝ TÊN MIỀN '.EU'

Khoảng 300.000 người châu Âu đã đổ xô đi đăng ký tên miền Internet mới '.eu' trong giờ đầu tiên cho phép đăng ký địa chỉ web site mới vào sáng ngày 7 tháng tư vừa qua. Phần lớn từ Anh, Đức, Hà Lan, Thụy Điển và Bỉ.

Tất cả các cơ quan luật pháp Châu Âu gồm: Uỷ Ban, Nghị viện châu Âu, Web Site chung của Châu âu sẽ chuyển sang tên miền '.eu' vào ngày 9 tháng 5 - ngày châu Âu.

Cơ quan đăng ký tên miền Internet của châu Âu - EURid- tổ chức phi lợi nhuận, vào giữa ngày đã báo cáo có 702.684 tên miền đã đăng ký. Số liệu thống kê do EURid cung cấp cho thấy, người Đức sở hữu 419.866 trong số 1.318.171 tên miền .eu đang hoạt động. Đứng ở vị trí thứ 2 trong bảng thống kê là Anh với 270.292 tên miền .eu .

Uỷ viên Uỷ ban châu Âu Viviane Reding nói: Uỷ ban hy vọng một ngày nào đó tên miền mới '.eu' trở nên đối thủ với tên miền .com. Từ bây giờ châu Âu và các công dân của nó có thể thiết kế các Web riêng của mình.

Các doanh nghiệp nhỏ của châu Âu cho rằng tên miền '.eu' sẽ có lợi cho các công ty châu Âu.

Các nhân viên EU nhắc nhở khách hàng chú ý rằng, phí đăng ký tổng thể chỉ là 12 euro (14,77 USD).

Quế Lâm

(Theo AP, BBC 07/04/2006)