La technologie GQ2 : Un complément essentiel à RSA

Une solution d'authentification

dynamique aussi sûre et plus rapide que le RSA

Plan de la présentation

- Introduction
- Présentation du protocole GQ2
- Analyse de sécurité du protocole GQ2
- Analyse des performances du protocole GQ2
- Expérience d'intégration du protocole GQ2
- Conclusion

Introduction

L'omniprésence du RSA

La saga de la sécurité des cartes bancaires

Du compromis … à la recherche d'un équilibre

Les résultats précédents .. Et nos résultats

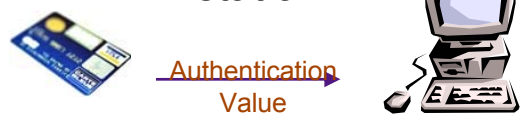
La technologie RSA

- **Une technologie découverte en 1977…**
  - Révolutionne le monde de la sécurité…
  - Reste sûre malgré 25 ans de recherche intensive
- **… qui domine actuellement le marché…**
  - Permet de mettre en œuvre la quasi-totalité des solutions de sécurité
    - Chiffrement, signature électronique, authentification, mise à la clé,…
  - Dispose d'une forte crédibilité scientifique
- **… mais dont le caractère "universel" à un prix**
  - Exemple : Comment mettre en œuvre une signature électronique et d'authentification dynamique dans des cartes à bas coût (sans crypto processeur), sans accroître la durée de la transaction, tout en apportant le niveau de confiance offert par RSA-1024.

La saga sécurité des CB

Le choix initial (1982): Authentification Statique RSA

- chip bon marché : pas de crypto processeur
- Transaction rapide : < 1 s pour une authentification
- Mais sécurité limitée : authentification statique



Les problèmes prédits apparaissent :

- En 1983, un module RSA de 320 bits : une sécurité moyenne (5 à 10 ans)
- En 1998, Humpich factorise le module : ouvre la porte aux “YES cards”

Une évolution discutable en 1999

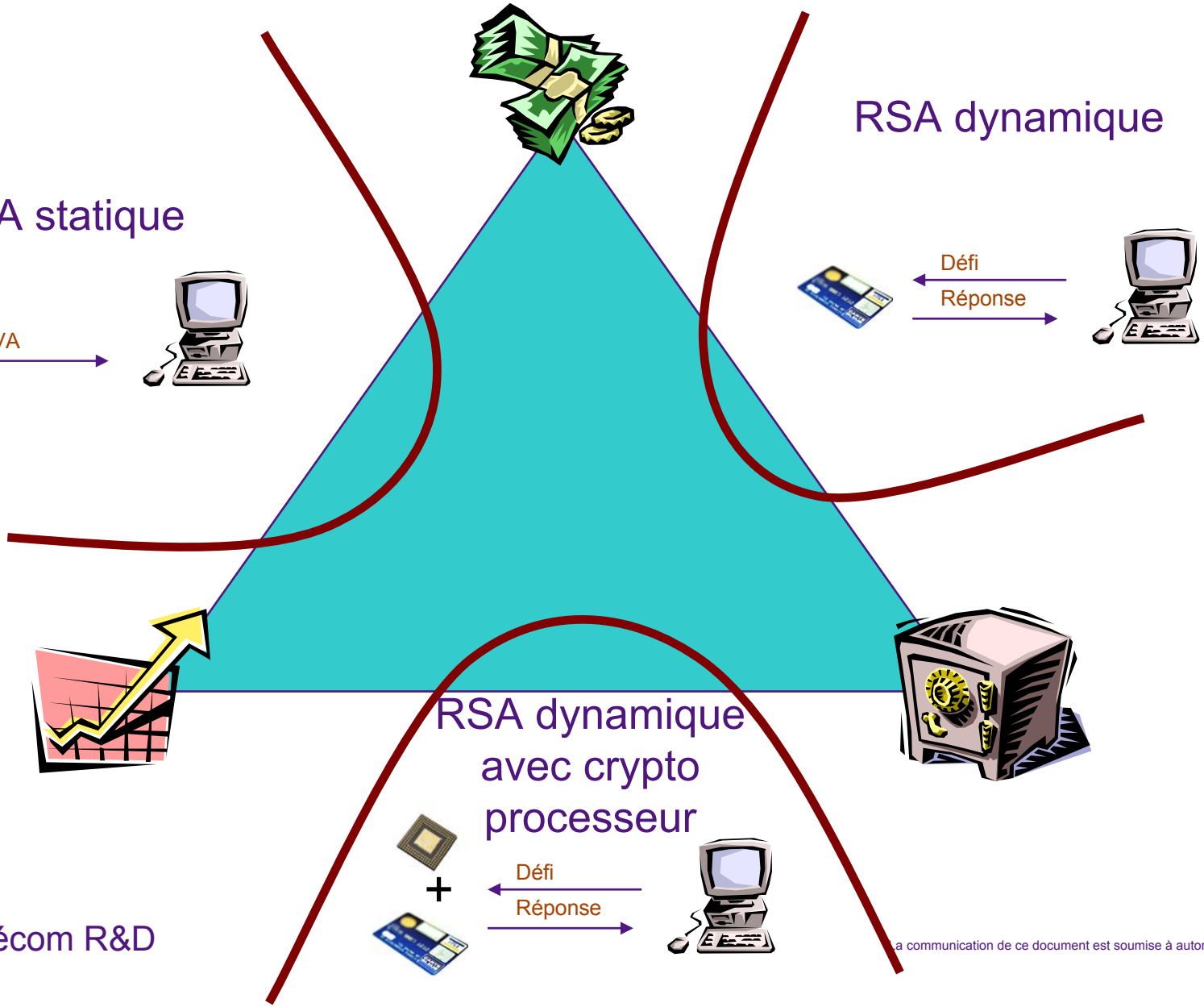
- Un module RSA de 768-bit : Non factorisé à ce jour
- Mais maintien d'une authentification statique : Possibilité de "clones".
  - Remboursement systématique en cas de fraude
  - Processus systématique ”on line” pour tout paiement automatique sans présence humaine.

Le chip n'est pas encore utilisé sur le NET

Du compromis …

- **Choisir une authentification statique plutôt qu'une authentification dynamique, ce qui permet le rejeu (Clone)**
- **Réduire la taille du paramètre de sécurité RSA, donc affaiblir la sécurité du système et par conséquent sa durée de vie**
- **Exploiter des solutions de sécurité non reliées à la technologie RSA (ex : NTRU, Sflash),**
  - Abandonner la référence à la factorisation dont la sécurité n'a jamais été démentie.
  - Se démarquer des PKI actuellement déployées et basées sur RSA

… à la recherche d'un équilibre



Les résultats précédents …

- **1987 : Protocole zero-knowledge de Fiat Shamir**
  - Sécurité basée sur le problème de la factorisation (racine carrée modulaire)
  - Performance affaiblie par le nombre important d'échange
- **1988 : Protocole zero-knowledge de Guillou Quisquater (GQ1)**
  - Sécurité basée sur le problème RSA (signature)
  - Diminution importante du volume d'échange entre le prouveur et le vérifieur
- **1990 : Protocole Ong Schnorr**
  - Sécurité basée sur les racines 2^k ième, mais n'est pas zero knowledge
  - Performance très proche de GQ1
- **2001 : Protocole Guillou Quisquater (GQ2)**
  - Performance optimale
  - Eléments de preuve sur l'équivalence avec le problème de la factorisation

… nos résultats

- **Preuve complète de la sécurité de GQ2, mise en évidence des conditions suffisantes du caractère ZK de GQ2**
  - En particulier, s'il existe un "algorithme" permettant à un attaquant de tromper un vérifieur, alors cet attaquant dispose d'un "algorithme" de factorisation
- **Etude comparative des performances de GQ2 avec les principaux protocoles d'autentification**
  - GQ2 offre les meilleurs ratios
- **Preuve expérimentale qu'une authentification dynamique dans une carte bancaire EMV est possible**
  - Sans l'ajout d'un crypto processeur,
  - En conservant la PKI déployée,
  - Sans impact significatif sur le temps de transaction
  - Avec une sécurité identique à un RSA-1024

Présentation du protocole GQ2

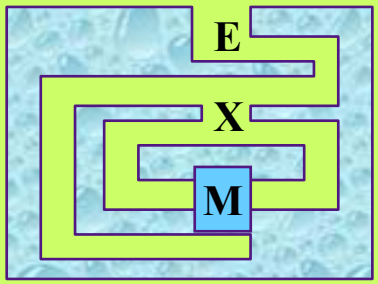
Présentation du zero knowledge

Les spécifications de GQ2

L'authentification GQ1, GQ2 et RSA

Zero-Knowledge

Prouver sans révéler le secret
Vérifier sans connaître le secret



La caverne magique

1. Claire et Véronique sont à l'entrée E
2. Seule Claire entre dans la caverne, jusqu'au point de rendez vous X. Alors, en se cachant de Véronique, elle s'engage au hasard dans l'un des couloir jusqu'à la porte magique M
3. Véronique entre alors à son tour jusqu'au point de rendez vous X et choisit au hasard l'un des deux couloirs puis défie Claire d'apparaître par le couloir choisi
4. Claire répond. Si nécessaire elle passe par la porte magique (en utilisant le mot de passe secret)
5. Véronique vérifie que Claire apparaît dans le couloir choisi
6. Claire et Véronique répète *l* fois les étapes 1 à 5.

Engagement / Challenge / Réponse / Vérification

GQ2: Génération de la bi-clé (ISO/IEC 9798-5)

Paramètres :

- k : Paramètre de sécurité
- m : Paramètre de multiplicité
- $\nu = 2^{k+1}$: Exposant de vérification

La clé publique GQ2:

- n : Module produit de deux grands nombres notés p_1 et p_2
- $G_1,\ldots,G_m$: Nombres publics tels que chaque G_i est le carré d'un petit nombre premier noté g_i appelé nombre de base. Pour au moins un nombre de base g on a $(g \mid p1) = -(g \mid p2)$

La clé privée GQ2:

- $Q_1,\ldots,Q_m$: Nombres secrets reliés au nombres publics par la relation for i from 1 to m $G_i \times Q_i^{\nu} \bmod n = 1$
- p_1 et p_2 : Deux grands nombres premiers vérifiant $p_1 = 3 \bmod 4$ et $p_2 = 3 \bmod 4$,

GQ2: le protocole d'authentification (ISO/IEC 9798-5)

- **Protocole entre deux parties : Un prouveur GQ2 (connaît Q) et un vérifieur (connaît G) partageant les paramètres k , $\nu=2^{k+1}$ et m**
- **Le prouveur GQ2 réalise systématiquement les étapes suivantes :**
  - Sélection d'un nombre aléatoire positif et inférieur n, noté r;
  - Calcul du nombre r^{ν} mod n, appelé engagement et noté W;
  - En réponse à tout challenge d consistant en m nombres aléatoires de k bits notés d1,…,dm, calcul du nombre $D=r \times Q_1^{d1} \times \ldots \times Q_m^{dm}$ mod n, appelé réponse et noté D;
  - Effacement du nombre aléatoire r;
- **Le vérifieur effectue systématiquement les étapes suivantes :**
  - Réception du prouveur de l'engagement W;
  - Sélection d'un challenge de m nombres aléatoires de k bits notés d1,..,dm;
  - A toute réponse D, calcul du nombre $W'=D^{\nu} \times G_1^{d1} \times \ldots \times G_m^{dm}$ mod n vérification que W=W' et W'<>0 et acceptation du prouveur;

GQ2 un exemple

Prouveur		Vérifieur
Certificat de la clé publique RSA <e,n> k=4 et m=2	CERTIFICAT →	Certificat de la clé publique RSA <e,n> k=4 et m=2
Deux nombres privées Q1 et Q2 : racines 32ième de 4 et 9 mod n		Deux nombres publics G1 et G2 : 4 et 9
Engagement: Nombre aléatoire $0 < r < n$ Calcul de $W = r^v \bmod n$	ENGAGEMENT →	W
(d1,d2)	CHALLENGE ←	Challenge : Deux quartets aléatoires d1 et d2
Réponse: Calcul de $D = r\, Q1^{d1}\, Q2^{d2} \bmod n$	VERIFICATION →	Vérification: Calcul de $W' = D^v G1^{d1}\, G2^{d2} \bmod n$ et test si W <>W'

Analyse de la sécurité du protocole GQ2

Attention MATHS ...

Le principal résultat

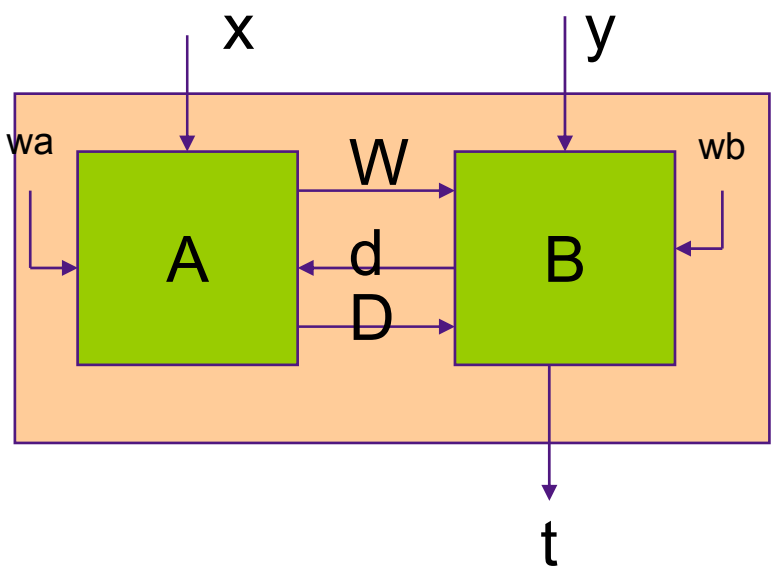
Les définitions du ZK

Résultat sur la sécurité du protocole GQ2

- **GQ2 est un protocole interactif à 3 passes**
- **GQ2 itéré à l'ordre l est une preuve zero-knowledge de connaissance de la factorisation du module sous les conditions suivantes:**
  - Le module n est de la forme p1 x p2 avec $p1 \equiv 3 \bmod 4$ et $p2 \equiv 3 \bmod 4$
  - Pour au moins un nombre de base g, $(g \mid p1) = -(g \mid p2)$
  - 2^{km} et l varient comme des polynômes en |n|
- **Equivalence avec la factorisation :**
  - la meilleure attaque pour tromper le vérifieur a une probabilité de réussite égale à 2^{-klm} (en général on prendra klm ~ 20)
  - S'il existe une attaque plus efficace c'est qu'il existe un algorithme polynomial de factorisation du module

Protocole interactif à trois passes

- **Couple de machines de Turing probabilistes A et B**
  - Utilisant des aléas locaux wa et wb
  - Recevant des données d'entrées : x,y
  - Echangeant des données internes : un triplet (W,d,D) noté Vue <A(x),B(y)>
  - Produisant une réponse binaire t notée <A(x),B(y)>
- **Si <A(x),B(y)> =1 on dit que A convainc B.**
- **GQ2 est un protocole à 3 passes**
  - Comme Fiat Shamir, Schnorr, GQ1, …



Quelques définitions …

P(Q,G) un prédicat : Q est appelé le témoin de G.

- Q ≡ (p1,p2) , G ≡ n , P(Q,G) ≡ " n est le produit de p1 par p2"

Un protocole interactif <A,B> est une preuve zero-knowledge de connaissance du prédicat P(Q,G) si :

- **Propriété de "consistance" (completeness):**
  - Pour tout G, si A connaît un témoin de G, alors A convainc B
- **Propriété de "significativité" (soundness) :**
  - Pour tout G, si un prouveur A* est capable de convaincre B avec une probabilité non négligeable alors il doit nécessairement connaître un témoin de G
- **Propriété de "sans connaissance" (zero-knowledge):**
  - Pour tout G, toute information obtenue par un vérifieur B* malhonnête au cours de l'exécution du protocole avec A peut être obtenue par B* sans interagir avec A.

"Aïe..." Voilà les maths ....

- **Un protocole interactif <A,B> est une preuve zero-knowledge de connaissance d'un prédicat P(Q,G) si :**
- **Propriété de "consistance" (completeness):**

$$\forall (G,Q)\ \ P(Q,G) \Rightarrow \Pr_{wa,wb}\left[\left\langle A_{wa}(Q), B_{wb}(G)\right\rangle\right] \geq 1 - e^{-|G|}$$

- **Propriété de "significativité" (soundness) :**

$$\forall c\ \exists M\ une\ \mathrm{MT}\ \forall \tilde{A}\ une\ MT\ \ \exists n_0\ \forall G / |G| > n_0$$

$$\Pr_{w\tilde{a},wb}\left[\left\langle \tilde{A}_{w\tilde{a}}(G), B_{wb}(G)\right\rangle\right] \geq \frac{1}{|G|^c} \Rightarrow \Pr_{wm}\left[P\left(M_{wm}(G), G\right)\right] \geq 1 - e^{-|G|}$$

- **Propriété de "sans connaissance" (zero-knowledge):**

$$\forall \tilde{B}\ une\ MT\ \exists M\ une\ MT \quad \forall (G,Q) / P(G,Q) \quad \forall (W,d,D)$$

$$\Pr_{wa,w\tilde{b}}\left[vue\left\langle A_{wa}(Q), \tilde{B}_{w\tilde{b}}(G)\right\rangle = (W,d,D)\right] = \Pr_{wm}\left[M_{wm}(G) = (W,d,D)\right]$$

Analyse des performances du protocole GQ2

Méthode d'analyse

Tableau comparatif des performances

Synthèse des performances

Analyse comparative

Critères de comparaison

- CM : Complexité de communication entre le vérifieur et le prouveur
- CPC : Complexité de calcul du prouveur
- CPV : Complexité de calcul du vérifieur
- CS : Stockage requis par le prouveur

Mesures d'évaluation

- Evaluation de CM et CS en Kbits
- Evaluation de CPC et CPV en nombre de multiplications modulaires

Résultats comparatives

Paramètres des protocoles Norme 9798-5 § C.4.3 (Module de 1024 bits)

	CS (K bits)	CPC	CPV	CM (K bits)
Fiat Shamir	5	11	11	8
GQ 1	2	33,5	21,5	2
GQ 2	5,5	7,75	3,75	2
Schnorr	2,31	200	208	1,17
RSA Unilateral Authentication	2,5	320	13	1,84
RSA Mutual authentication	2,5	333	333	2,42

Performances de GQ2

Services offerts par GQ2 :

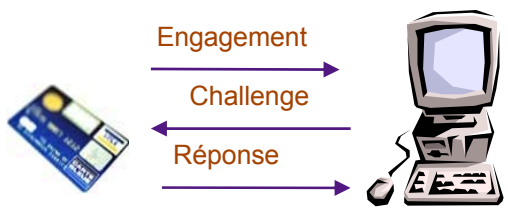
- Services d'intégrité (authentification et signature électronique)
- Pas de services de confidentialité (chiffrement, mise à la clé)

Sécurité physique de GQ2

- Quand RSA utilise un secret comme exposant (public ^{secret} mod n), GQ2 utilise le secret comme argument (secret ^{public} mod n)
- La "power analysis" est plus difficile avec GQ2 qu'avec RSA

RSA / GQ2

- En dépit d'une étape supplémentaire dans le protocole (résultant du caractère ZK) et d'une taille de clé plus grande, GQ2 réduit considérablement le temps de calcul par rapport à RSA.



GQ2

Expérience d'intégration du protocole GQ2

Comparaison avec le RSA

Authentification dynamique dans une carte EMV-SDA

Comparaison RSA / GQ2

- **Authentification dynamique et signature comparées d'une carte à puce, intégration réalisée en collaboration avec EDSI**

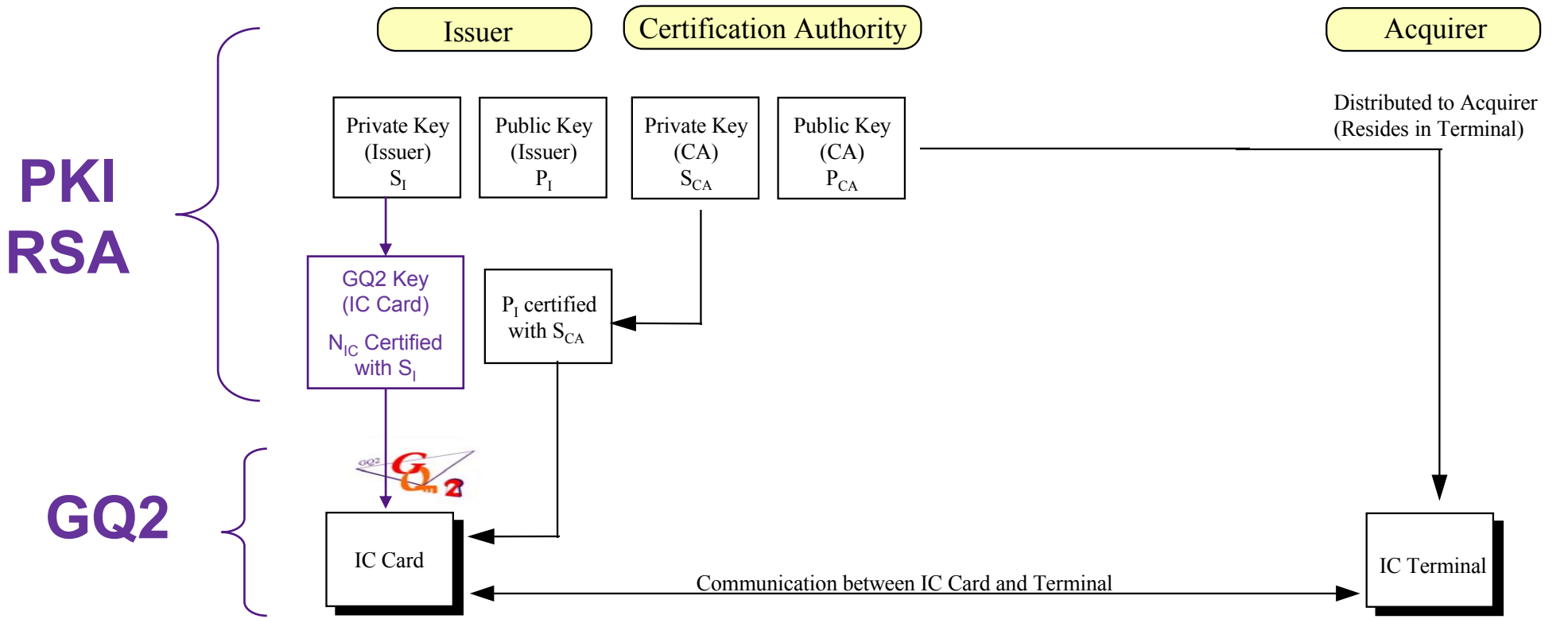
- **Caractéristiques de la démonstration**
  - Même module (1024 bits)
  - Même librairie de programmes
  - Même carte à puce
    - Processeur ATMEL, 4Mhz
    - sans utilisation du crypto-processeur
- **Résultat : Moyenne du rapport temps authentification RSA/GQ2 = 40 et signature RSA/ GQ2 = 12**

Authentification dynamique EMV-SDA

- **Carte bancaire EMV; intégration des logiciels par EDSI**
- **Terminal de paiement bancaire de Thalès et Ingenico; intégration des logiciels par Sim@Bay**
- **Authentification dynamique GQ2 suivie d'une transaction EMV**
- **Caractéristiques de la démonstration**
  - Un module de 1024 bits par carte
  - Puce sans crypto-processeur
- **Résultat : allongement imperceptible du temps d transaction**
  - Authentification GQ2 : de 1 s à 1,5 s
  - Temps global de la transaction : 20 s

SIM@BAY

Intégration de GQ2 dans EMV



Card provides to terminal :

- P_I certified by Certification Authority
- Card data with digital signature

- Including N_{IC}

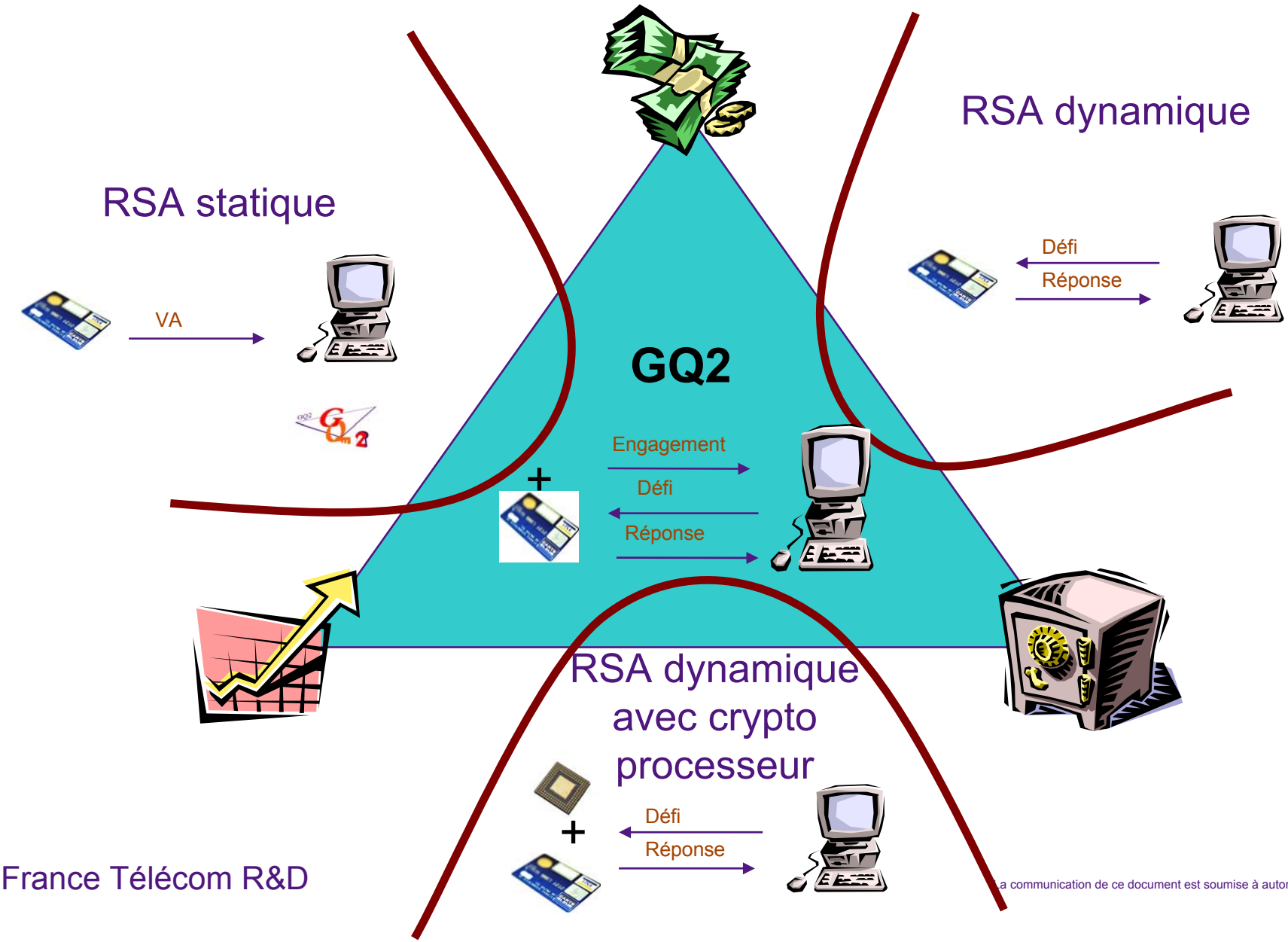
Terminal :

- Uses P_{CA} to verify that the Issuer's P_I was certified by the CA
- Uses P_I to verify the digital signature of the card data

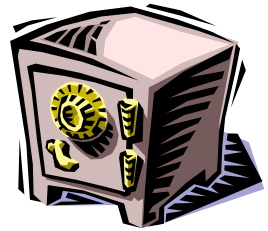
- Use N_{IC} for GQ2 dynamic authentication

Conclusion

GQ2 : permet l'équilibre



Synthèse comparative

	GQ2	RSA
Sécurité 	**Problème de la factorisation du module** ▸ Exactement équivalent ▸ Zero knowledge	▸ Presque équivalent
	X^Y mod Z et l'analyse de la consommation ▸ X est secret ▸ Facile à protéger	▸ Y est secret ▸ Difficile à protéger
Efficacité 	**X^Y mod Z et les performances** ▸ Y est petit, Calcul très rapide ▸ Auth. De 1 s (modulo de 1024 bits)	▸ Y est grand, Calcul lent ▸ Auth. de 40 s (modulo de 1024 bits)
Coût 	**Intégration** ▸ Possible avec un composant sans crypto-processeur ▸ S'appuie sur les bibliothèques nécessaires pour le RSA	▸ Exige un composant à crypto-processeur
	Exploitation ▸ Paramètrable: s'adapte aux exigences des services	▸ peu paramètrable (taille modulo)

Merci

Eléments de preuve 1/2

Prédicat associé à GQ2 :

- G = (n,G1,…,Gm) , Q=(n,Q1,…Qm)
- P(Q,G) ≡ (pour tout i:1,…,m $G_iQ_i^{\nu}=1 \bmod n$)
- Ce prédicat est équivalent à celui associé au problème de la factorisation

Propriété "Soundness" de GQ2:

- Si un attaquant A* peut convaincre B avec une probabilité non négligeable (PNN) alors il peut produire avec une PNN des triplets (W,d,D) valides
- On montre (théorème général) que dans ce cas il peut aussi produire avec une PNN des couples de triplets valides de la forme (W,d,D) , (W,e,E) avec d <> e (appelés alors triplets entrelacés)
- On montre (dans le cas particulier de GQ2) que la connaissance de triplets entrelacés conduit avec une chance sur 2 à la factorisation du module

Eléments de preuve 2/2

- **Propriété "Completeness" de QG2 :**
  - Trivial par construction
- **Propriété "zero knowledge" de GQ2:**
  - Dans le cas particulier de GQ2, on montre que pour tout triplet valide il existe un mode public et un mode privé de génération (dualité des triplets)
  - Dans le cas général, on montre alors que l'existence d'une telle dualité permet de simuler toute interaction entre le prouveur honnête A et un vérifieur malhonnête B* (quelque soit sa stratégie)
  - Toute connaissance acquise de l'interaction entre A et B* peut être obtenue entre A* et B* ne connaissant pas le secret de A
  - L'interaction entre A et B* ne peut donc pas laisser fuir d'information sur le secret de A

Synthèse des propriétés de GQ2

Protocole GQ2 non itéré (l=1)

- GQ2 possède la propriété de completeness
- Si log(|n|)=o(km) alors GQ2 possède la propriété de soundness
- Si 2^{km} est polynomial en n alors GQ2 possède la propriété de zero knowledge (égalité des deux lois)
- Attention les deux conditions sont contradictoires.

Protocole GQ2 itéré (paramètre l) :

- GQ2 possède la propriété de completeness
- Si log(|n|)=o(klm) alors GQ2 possède la propriété de soundness
- Si l et 2^{km} sont polynomiaux en n alors GQ2 possède la propriété de zero knowledge
- Les deux conditions ne sont plus contradictoires.