

# CRYPTO RUMP NEWS

Norris Center for the Performing Arts, 27570 Crossfield Drive in RHE, on Saturday, March 20 at 2 and 4 p.m. Tickets are \$38 for adults and \$19 for students for the evening performance and \$30 for adults and \$15 for students at the matinee performance. For reservations, call 544-0403.

• **UPCOMING** — The Palos Verdes Peninsula Unified School District and Friends of School Music host the 15th Palos Verdes Elementary Choral Festival on March 23, 24 and 25 at the Norris Center for the Performing Arts, 27570 Crossfield Drive in RHE. All shows begin at 7:30 p.m. For tickets, call the Norris box office at 544-0403.

• **ONGOING** — The Distinctive Edge, 29050 S. Western Ave., Suite 113 in RPV, continues "Third Time's a Charm," an exhibit of 3-D collages by artist Steve Jacobsen, through March 30. For gallery hours, call 833-3613.

• **ONGOING** — "Natural Treasures" exhibition contin-

## Breaking news in ecash: efficient & provably secure ecash implemented!

Two years ago, U.S. Navy personnel and their families assigned to the Atsugi Navy base, home of the U.S.S. Kittyhawk, were treated to a rare

teacher and assistant director of the Orange County Symphony; and Mike Tiffany, bass, a computer engineer. The band has been playing the length

south of Tokyo — left the home away from home, with its lush green rolling landscape and its multitude of cherry blossom trees. "Yet," Fleming says, "our was struck by the commitment and dedication of our men and women in uniform as they played their part in protecting and serving in an ever challenging and hostile world."

A couple of the families even took time out from their busy schedule to host Terry and the band members. They treated them to a guided tour of the base and accompanied them on a few exciting trips off the base, visiting beautiful ancient temples, monuments and revered giant Buddhas.

On a visit to downtown Tokyo, the band came across what they assumed was a very rare sight, a place called "Scruffy Murphy," an Irish pub located in the heart of a bustling downtown. Upon checking the establishment out, they discovered a real authentic Irish Pub with excellent Guinness and good pub grub. It also happened to be open mic night, so the band members took over the stage

and entertained the locals for a few fun-filled hours. It turned out that it was just one of many establishments in the city.

A special bond developed between the band members and these families and already exchange visits have occurred when the same families were on leave in the United States.

For more information about the band, log on to [www.bvnsigfreemusic.com](http://www.bvnsigfreemusic.com).



Even though far from home, the Atsugi base — situated a few hours

**thebridge**

**THE BRIDGE** (ON THE BRIDGE)  
 THE BRIDGE AT VERNON HAVEN CENTER • OFFICE  
 2001 • 1000 HAVEN AVENUE • VERNON HAVEN • THE BRIDGE  
 AT VERNON HAVEN CENTER

**ALL SHOWS 10:00 AM • ALL SHOWS 10:00 AM**  
 Purchase Tickets by phone at 215-563-3379  
 or online at [www.thebridgeatvernon.com](http://www.thebridgeatvernon.com)  
 Contact us at 215-563-3379

**SPECIAL STUDENT PRICE WITH US \$1.00**

**REGULAR SEATING 10:00 AM**

**SEATING LEVELS (20 SEAT PREMIUM SEATING & 1000 SEAT)**  
 SEATING LEVELS (20 SEAT PREMIUM SEATING & 1000 SEAT)  
 2:15 4:15 7:15 9:15 11:15 1:15  
 \* SEATING & AREA 12:45 3:15 5:15 7:15 9:15

**SEATING (20 SEAT PREMIUM SEATING & 1000 SEAT)**  
 12:45 3:15 5:15 7:15 9:15 11:15

**AGENT GUY BANGS IN DISTRIBUTION (2000 SEAT)**  
 12:45 3:15 5:15 7:15 9:15 11:15

**SEATING AND SEATING (20 SEAT)**  
 12:45 3:15 5:15 7:15 9:15 11:15

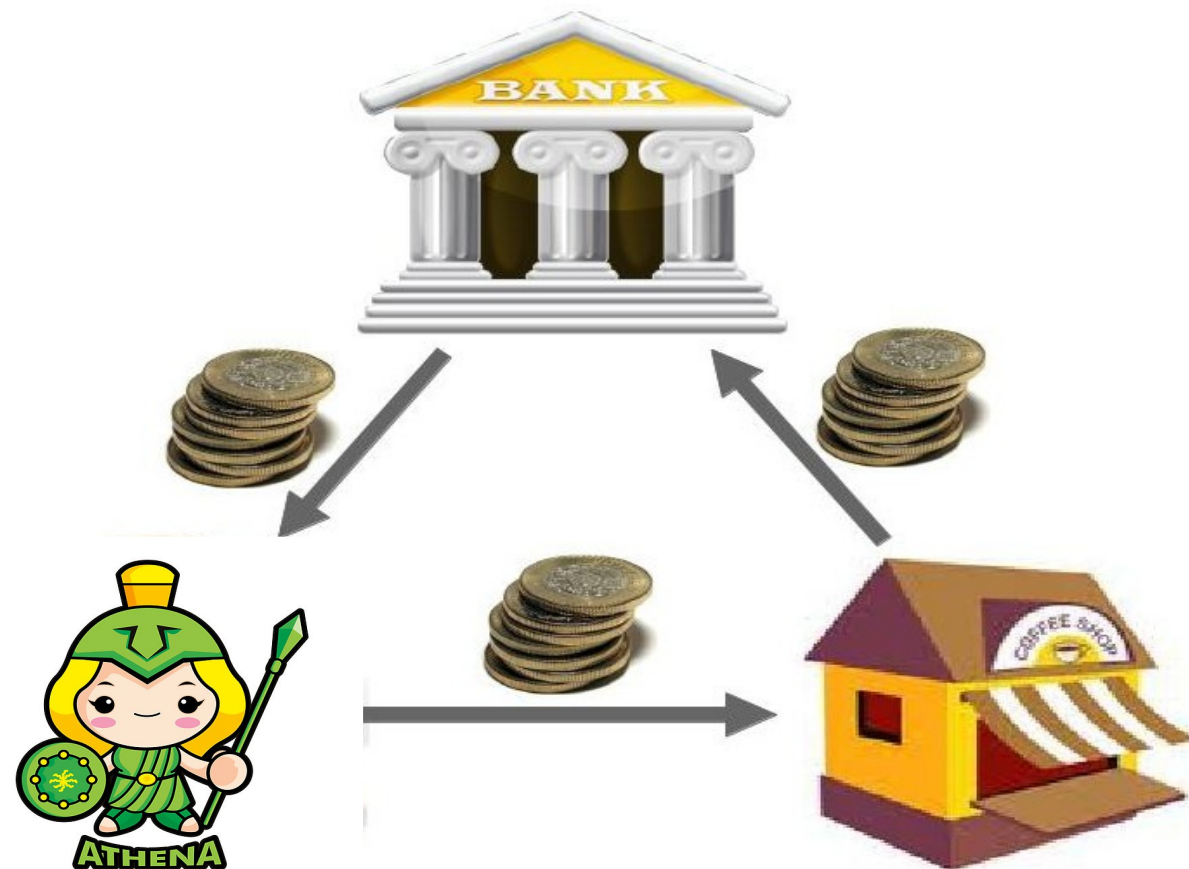
• **RESERVATION 215-563-3379**

## Foteini Baldimtsi

Joint work with: Anna Lysyanskaya, Gesine Hinterwälder, Christian T. Zenger, Wayne P. Burleson, Christof Paar



# Cryptographic e-cash



**Anonymous**

# State of the art

Chaum'81, Chaum'82, CFN'90, FY'93, Brands'93, CPS'94, FTY'96, Tsiounis'97, CHL'05,.....

Brands'93: Most efficient, well known and widely implemented.



# State of the art

Chaum'81, Chaum'82, CFN'90, FY'93, Brands'93, CPS'94, FTY'96, Tsiounis'97, CHL'05,.....

Brands'93: Most efficient, well known and widely implemented.



Brands ecash cannot be proven unforgeable under any assumption (including one-more type assumptions) using standard RO proof techniques [BL'12a]



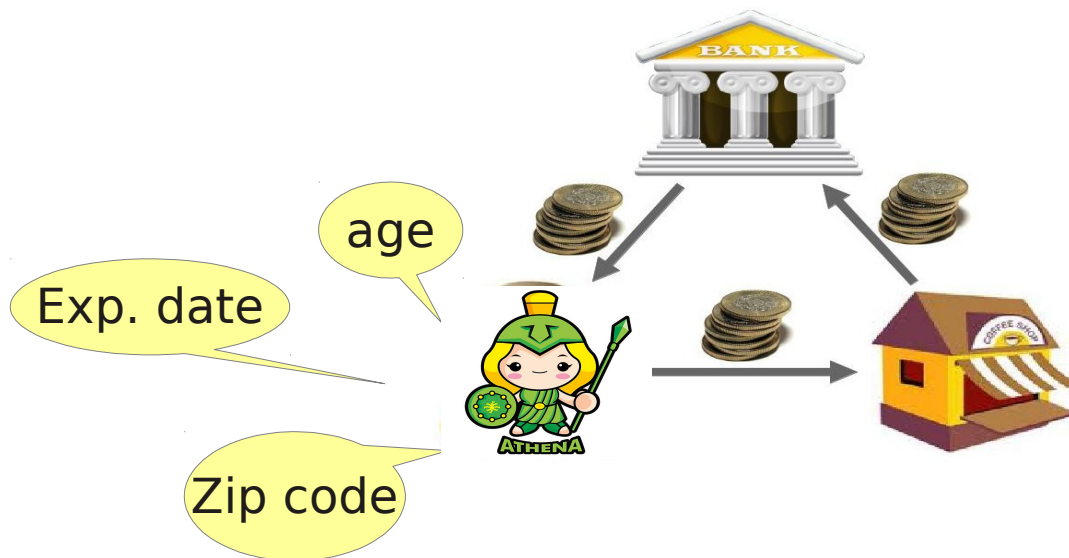
Good News  
Everyone!



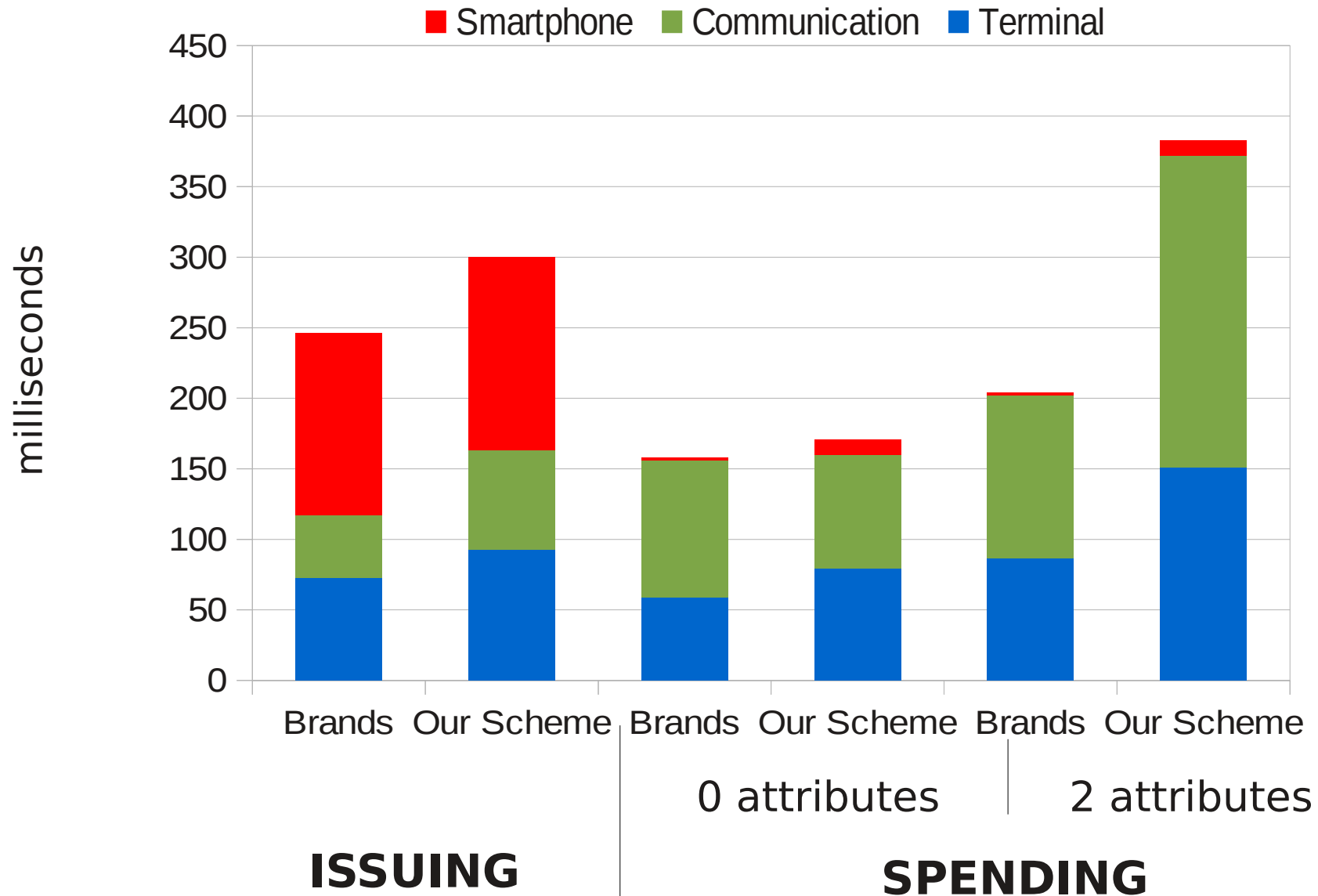
# Efficient e-cash with attributes

“Anonymous Credentials Light” [BL'12b] → e-cash.

- ◆ Comparably efficient to Brands
- ◆ Provably secure in the RO model under the DDH assumption
- ◆ Allows the encoding of attributes



# Performance Results





# References

**“On the Security of One-Witness Blind Signature Schemes”**, [Foteini Baldimtsi](#) and Anna Lysyanskaya, Cryptology ePrint Archive, Report 2012/197

**“Anonymous Credentials Light”**, [Foteini Baldimtsi](#) and Anna Lysyanskaya, Cryptology ePrint Archive, Report 2012/298

**“Efficient E-cash in Practice: NFC-based Payments for Intelligent Transportation Systems”**, Gesine Hinterwalder, Christian T. Zenger, [Foteini Baldimtsi](#), Anna Lysyanskaya, Christof Paar and Wayne P. Burleson, Privacy Enhancing Technologies Symposium - PETS, 2013.

